COMTREND CORPORATION

CT-5621T

ADSL2+ Multi-port Router

User's Manual

Version A3.2, November 23, 2007

261055-015

Warning

- Before servicing or disassembling this equipment, always disconnect all power and telephone lines from the device
- Use an appropriate power supply and a UL Listed telephone line cord. Specification of the power supply is clearly stated in Appendix C

Preface

This manual provides information to network administrators. It covers the installation, operation and applications of the ADSL2+ multi-port router.

The individual reading this manual is presumed to have a basic understanding of telecommunications. For product update, new product release, manual revision, software upgrade, technical support, etc., visit Comtrend Corporation at http://www.comtrend.com

This document is subject to change without notice.

Copyright

Copyright© 2007 Comtrend Corporation. All rights reserved. The information and messages contained herein are proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written permission by Comtrend Corporation.

Technical support

If you find the product to be inoperable or malfunctioning, please contact a technical support engineer for immediate service by email at INT-support@comtrend.com

Table of Contents

CHAPTER 1 INTRODUCTION 5

1.1 FEATURES 5

1.2 APPLICATION 6

1.3 FRONT PANEL LED INDICATORS 7

CHAPTER 2 INSTALLATION 9

2.1 HARDWARE INSTALLATION 9

2.2 USB DEVICE DRIVER AUTO-RUN INSTALLATION 11

2.3 USB DRIVER MANUAL INSTALLATION (64BIT OS) 14

CHAPTER 3 LOGIN VIA THE WEB BROWSER 19

3.1 IP ADDRESS 20

3.2 LOGIN PROCEDURE 21

3.3 DEFAULT SETTINGS 23

CHAPTER 4 DEVICE INFO 24

4.1 WAN 25

4.2 STATISTICS 26

4.2.1 LAN Statistics 27

4.2.2 WAN Statistics 28

4.2.3 ATM statistics 29

4.2.4 ADSL Statistics 31

4.2.5 Route 33

4.2.6 ARP 33

4.2.7 DHCP 34

CHAPTER 5 QUICK SETUP 35

5.1 AUTO QUICK SETUP 36

5.2 MANUAL QUICK SETUP 37

5.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) 39

5.2.2 MAC Encapsulation Routing (MER) 44

5.2.3 IP Over ATM 47

5.2.4 Bridging 51

CHAPTER 6 ADVANCED SETUP 53

6.1 WAN 55

6.2 LAN 56

6.3 NAT 58
6.3.1 Virtual Servers *58*
6.3.2 Port Triggering *60*
6.3.3 DMZ Host *61*
6.3.4 ALG *62*
6.4 SECURITY 63
6.4.1 IP Filtering *63*
6.4.2 Parental Control *66*
6.4.3 MAC Filtering *67*
6.5 QUALITY OF SERVICE 69
6.6 ROUTING 72
6.6.1 Default Gateway *72*
6.6.2 Static Route *73*
6.6.3 RIP *74*
6.7 DNS 75
6.7.1 DNS Server *75*
6.7.2 Dynamic DNS *76*
6.8 DSL 78
6.9 PORT MAPPING 79
6.10 CERTIFICATE 82
6.10.1 Local *82*
6.10.2 Trusted CA *84*

CHAPTER 7 DIAGNOSTICS 85

CHAPTER 8 MANAGEMENT 87

8.1 SETTINGS 87
8.1.1 Configuration Backup *88*
8.1.2 Update Settings *89*
8.1.3 Restore Default *90*
8.2 SYSTEM LOG 92
8.3 TR-069 CLIENT 95
8.4 INTERNET TIME 97
8.5 ACCESS CONTROL 98
8.5.1 Services *99*
8.5.2 Access IP Addresses *100*
8.5.3 Passwords *101*
8.6 UPDATE SOFTWARE 102
8.7 SAVE AND REBOOT 103

APPENDIX A: FIREWALL 104

APPENDIX B: PIN ASSIGNMENTS 110

APPENDIX C: SPECIFICATIONS 111

APPENDIX D: SSH CLIENT 113

Chapter 1 Introduction

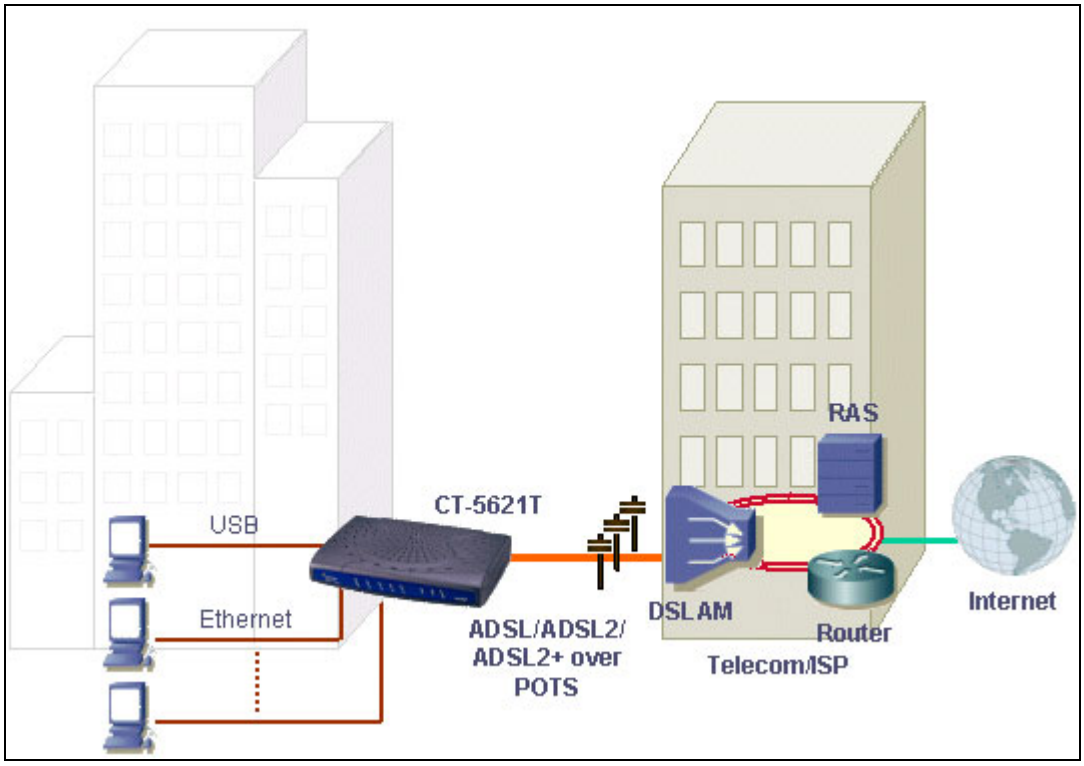
The CT-5621T is an ADSL router with four 10/100 Base-T Ethernet ports and a single USB port providing wired LAN connectivity. The CT-5621T ADSL2+ multi-port router provides state of the art security features such as Firewall and VPN passthrough. The CT-5621T is designed for both residential and business applications that require wired connectivity to an ADSL broadband network. The CT-5621T supports up to 16 contiguous virtual connections, allowing for multiple simultaneous connections.

1.1 Features

- UPnP
- RADIUS client
- IP /MAC address filtering
- Static route/RIP/RIP v2 routing functions
- Dynamic IP assignment
- IP QoS
- NAT/PAT
- IGMP Proxy
- DHCP Server/Relay/Client
- DNS Proxy
- Auto PVC configuration
- Per-VC packet level QoS
- Up to 16 VCs
- Web-based management
- Remote configuration and upgrade
- Configuration backup and restoration
- FTP server
- TFTP server
- TR-069
- TR-068

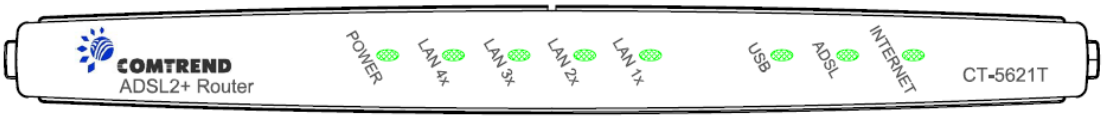
1.2 Application

The following diagram depicts the application of the CT-5621T multi-port router.



1.3 Front Panel LED Indicators

The front panel LED indicators are pictured below. The table that follows provides detailed explanations of their function.



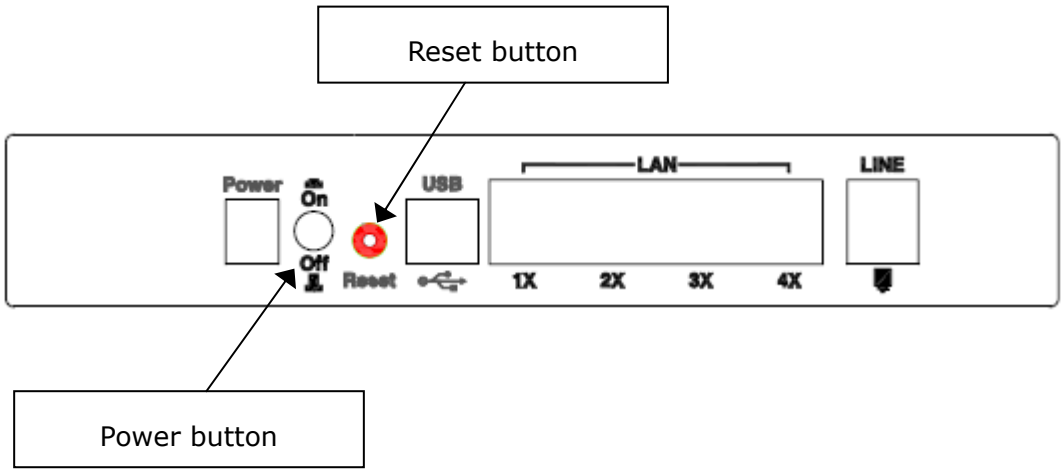
LED	Color	Mode	Function
POWER	Green	On	The router is powered up.
		Off	The router is powered down.
	Red	On	POST (Power On Self Test) failure (not bootable) or Device malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data. This may be identified at various times such after power on or during operation through the use of self testing or in operations which result in a unit state that is not expected or should not occur.
LAN 4x~1x	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
	Green	Blink	Data transmitting or receiving over LAN.
USB	Green	On	A USB link is established.
		Off	A USB link is not established.
	Green	Blink	Data transmitting or receiving over USB.
ADSL	Green	On	DSL good sync
		Off	Modem power off
	Green	Blink	Flashing Green = DSL attempting sync Flashing at 2 Hz with a 50% duty cycle when trying to detect carrier signal Flashing at 4 Hz with a 50% duty cycle when the carrier has been detected and the modem is trying to train.

INTERNET	Green	On	IP connected and no traffic detected.
		Off	Modem power off, modem in bridged mode or ADSL connection not present.
	Green	Blinking	IP connected and IP Traffic is passing thru the device (either direction)
	Red	On	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.) For bridged mode, the indicator light is off. If the IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present. If the session is dropped for any other reason, the light is turned off. The light will turn red when it attempts to reconnect and DHCP or PPPoE fails.

Chapter 2 Installation

2.1 Hardware Installation

In the rear panel, there is a reset button. To load the factory default settings, hold the reset button down for at least 5 seconds.



Follow the instructions below to complete the hardware connections.

Connection to LINE port

If you wish to connect both the router and a telephone, connect the LINE port to a POTS splitter with a RJ11 connection cable.

Connection to LAN port

To connect to a hub or PC, use a RJ45 cable. You can connect the router to up to four LAN devices. The ports are auto-sensing MDI/X and either straight-through cable or crossover cable can be used.

Connection to USB port

Connect the USB port to a PC with a standard USB cable.

Connection to Power

Connect the **Power** jack to the shipped power cord. Attach the power adapter to the wall outlet or other AC source. After all connections have been made, press the power-switch in to turn the device on. After power on, the router performs a self-test. Wait for a few seconds until the test is finished, then the router will be ready to operate.

Caution 1: If the router fails to power up, or it malfunctions, first verify that the power supply is connected correctly. Then power it on again. If the problem persists, contact our technical support engineers.

Caution 2: Before servicing or disassembling this equipment always disconnect all power cords and telephone lines from the wall outlet.

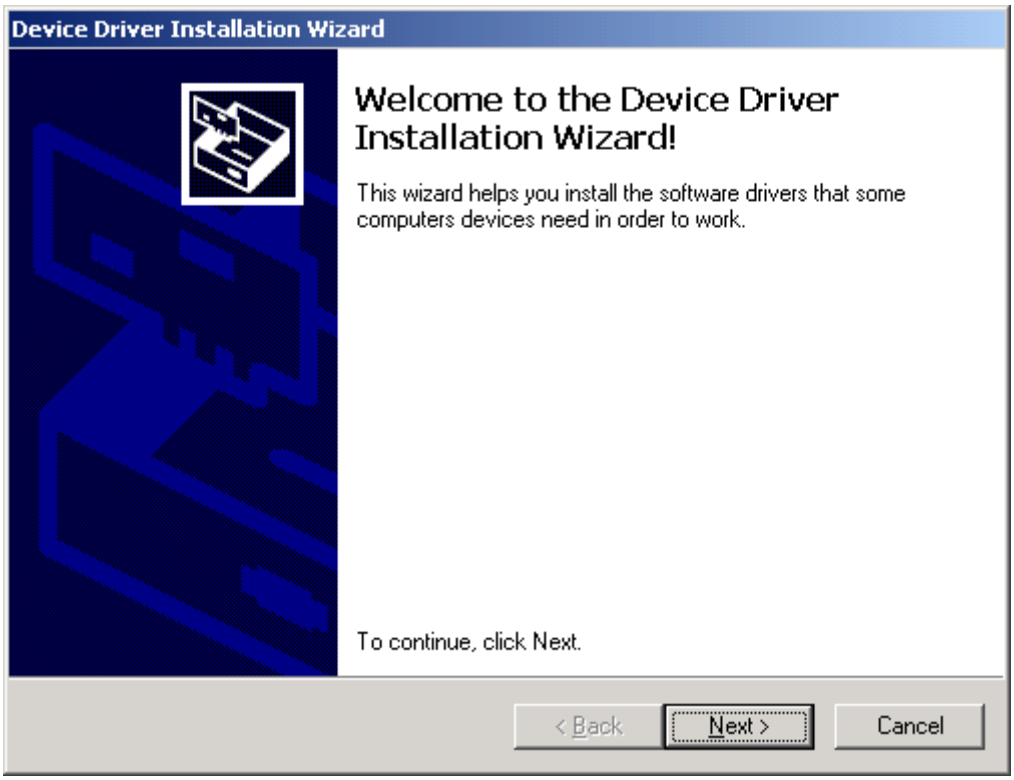
2.2 USB Device Driver Auto-run Installation

Before you connect your router's USB cable to your PC, you must load the ADSL USB drivers. The auto-run USB driver installation supports Win ME, Win 98, Win 2000, Win XP (32 bit) and Vista (32 bit). For those using Windows XP 64 bit, the driver needs to be installed manually (please see section 2.3 below for details), and the driver is also enclosed on the CD-ROM.

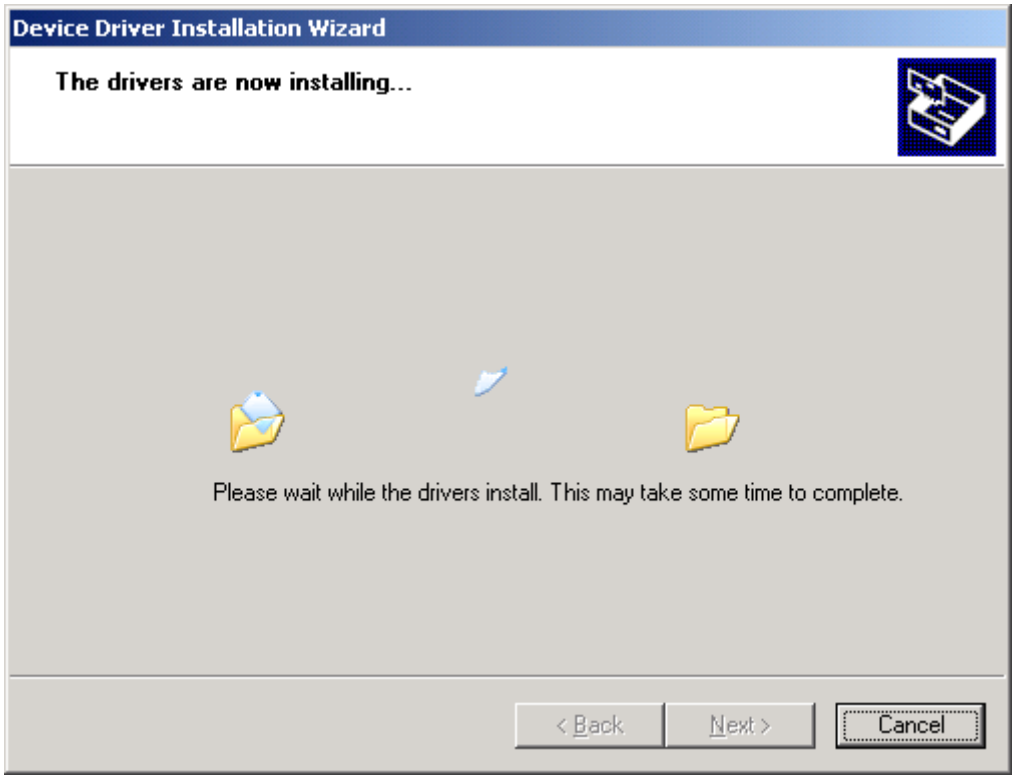
To connect the router to a PC using the USB interface, you need to use a standard USB cable and install the USB interface software. Follow the steps below:

STEP 1: Insert the Installation disk and select the **Install USB Driver** option.

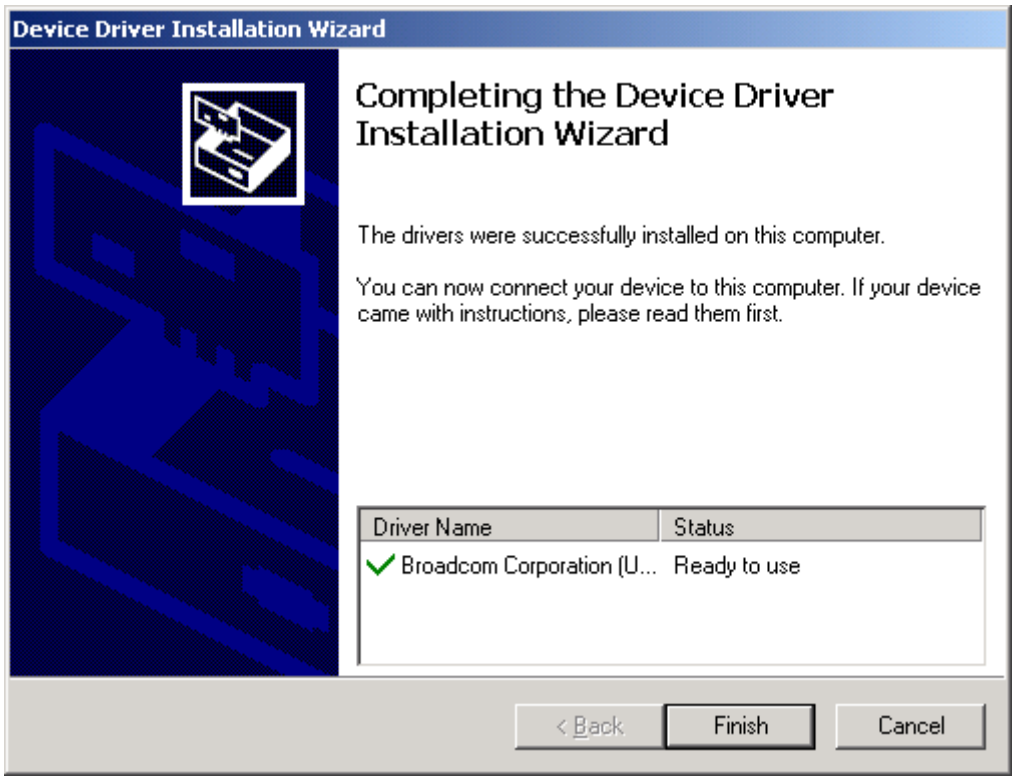
STEP 2: The following screen will be displayed. Click the **Next** button to continue.


Device Driver Installation Wizard
Welcome to the Device Driver Installation Wizard!
This wizard helps you install the software drivers that some computers devices need in order to work.
To continue, click Next.
< Back
Next >
Cancel

STEP 3: When the screen displays as below, wait until the drivers are fully installed.


Device Driver Installation Wizard
The drivers are now installing...
Please wait while the drivers install. This may take some time to complete.
< Back
Next >
Cancel

STEP 4: Click the **Finish** button, when the screen displays as below.


Device Driver Installation Wizard
Completing the Device Driver Installation Wizard
The drivers were successfully installed on this computer.
You can now connect your device to this computer. If your device came with instructions, please read them first.
Driver Name
Status
Broadcom Corporation (U...
Ready to use
< Back
Finish
Cancel

STEP 5: Installation is complete.

2.3 USB Driver Manual Installation (64bit OS)

Before you connect your router's USB cable to your PC, you must load the ADSL USB drivers. This manual USB driver installation supports Windows XP 64 bit.

To connect the router to a PC using the USB interface, you need to use a standard USB cable and install the USB interface software. Follow the steps below:

STEP 1: Connect the USB router to the PC by plugging the flat connector of a standard USB cable into your PC, and plugging the square connector into the router. The screen will display as below:

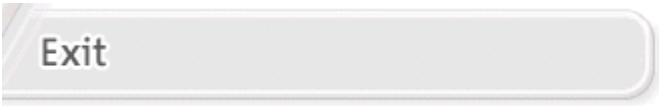
STEP 2: When the screen displays as below, select **install from a list of specific location (Advanced)** and click the **Next** button.

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
This wizard helps you install software for:
USB Network Interface
If your hardware came with an installation CD or floppy disk, insert it now.
What do you want the wizard to do?
Install the software automatically (Recommended)
Install from a list or specific location (Advanced)
Click Next to continue.
< Back
Next >
Cancel

Note: This screen won't be displayed if the USB Driver has been previously un/installed.

STEP 3: If you are installing the software from a disk, insert the disk.

Note: When the auto-run screen pops up click **Exit** and continue with the manual installation process (see below).

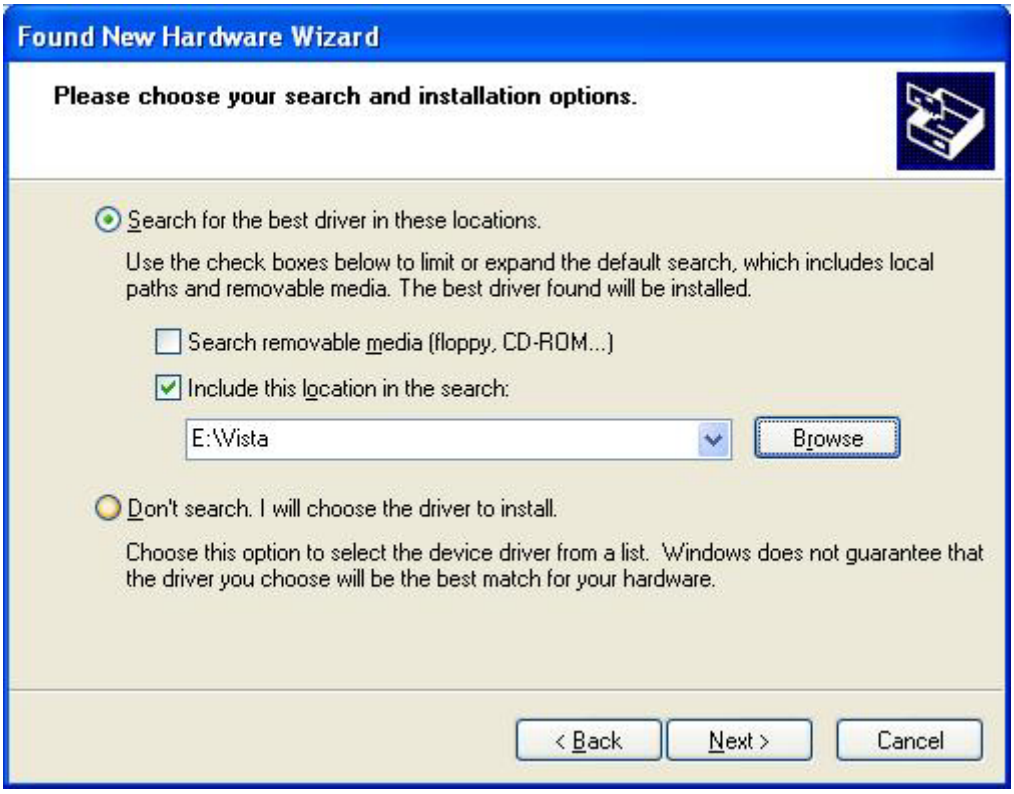


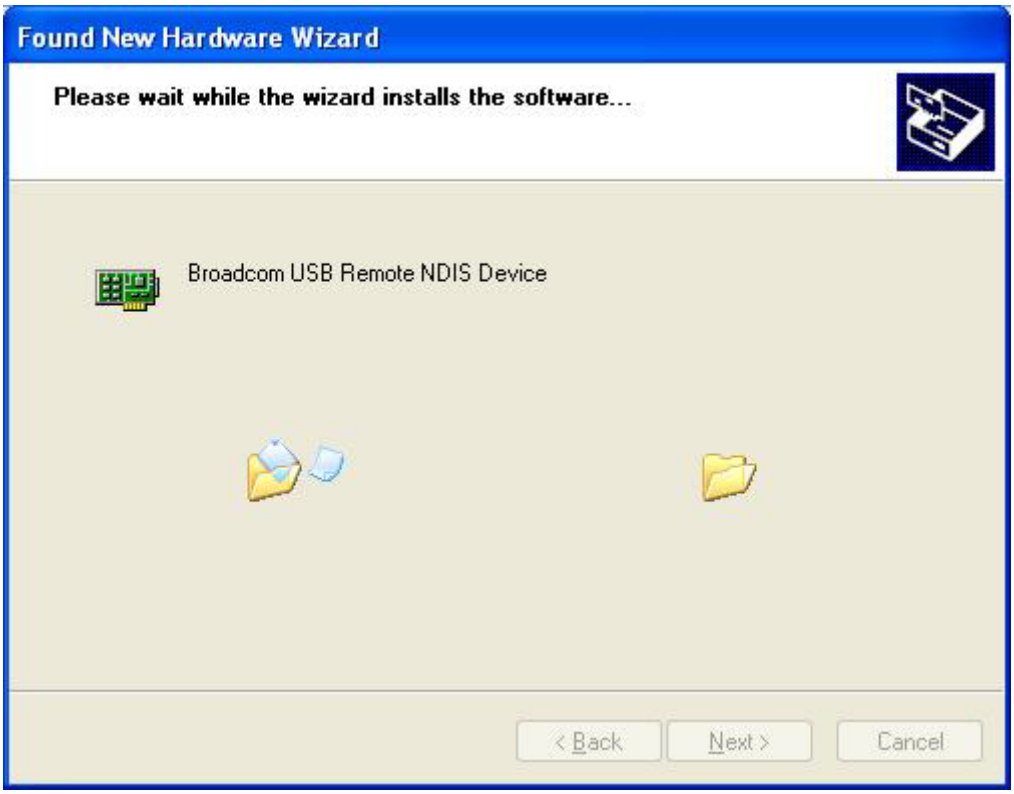
Found New Hardware Wizard
Please choose your search and installation options.
Search for the best driver in these locations.
Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.
Search removable media (floppy, CD-ROM...)
Include this location in the search:
Browse
Don't search. I will choose the driver to install.
Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.
< Back
Next >
Cancel

STEP 4: Select the location of the file using the **Browse** button. Normally, the file is on the CD-ROM shipped with the device.

STEP 5: Locate the **Vista** folder, and click the **OK** button.

STEP 6: When the screen displays as below, click the **NEXT** button.


Found New Hardware Wizard
Please choose your search and installation options.
Search for the best driver in these locations.
Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.
Search removable media (floppy, CD-ROM...)
Include this location in the search:
E:\Vista
Browse
Don't search. I will choose the driver to install.
Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.
< Back
Next >
Cancel



STEP 7: Click the **Finish** button, when the screen displays as below.

Found New Hardware Wizard
Completing the Found New Hardware Wizard
The wizard has finished installing the software for:
Broadcom USB Remote NDIS Device
Click Finish to close the wizard.
< Back
Finish
Cancel

STEP 8: Installation is complete.

Chapter 3 Login via the Web Browser

You can use a web browser, such as Microsoft Internet Explorer, to access the device remotely. The web-based user interface is best viewed with Microsoft Internet Explorer (version 5.0 and later).

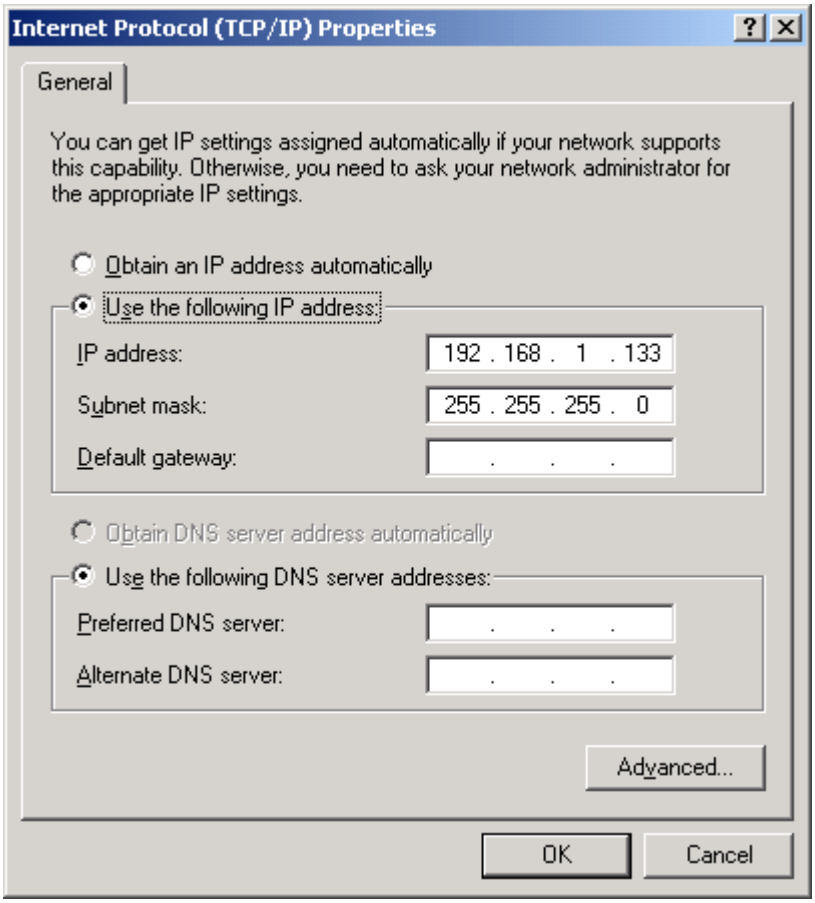
The default user account is assigned with user name **root** and password **12345**. The user can change the default password later when logged in to the device.

3.1 IP Address

The default IP address of the CT-5621T (LAN port) is 192.168.1.1. To configure the CT-5621T for the first time, the configuration PC must have a static IP address within the 192.168.1.x subnet. Follow the steps below to configure your PC IP address to use subnet 192.168.1.x.

STEP 1: Right click on the Local Area Connection under the Network and Dial-Up connection window and select Properties.

STEP 2: Enter the TCP/IP screen and change the IP address to the domain of 192.168.1.x/24.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 133
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

STEP 3: Click **OK** to submit the settings.

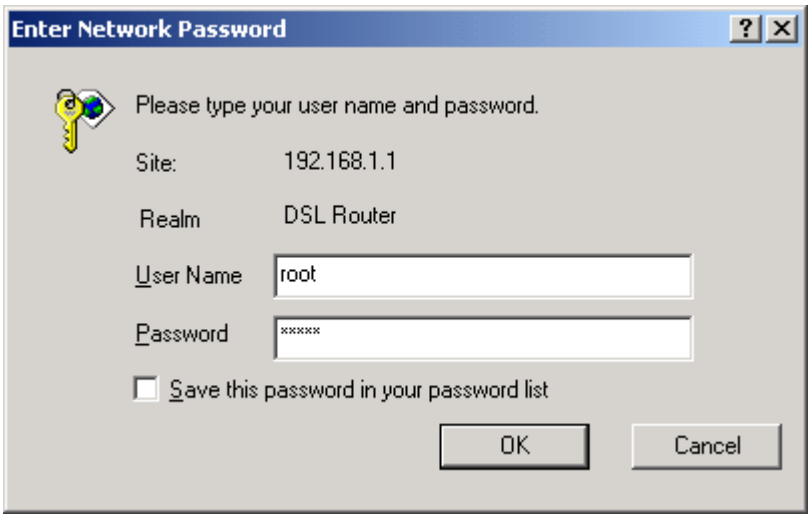
STEP 4: Start your Internet browser and type the IP address for the router (192.168.1.1) in the Web address bar.

3.2 Login Procedure

Perform the following steps to bring up the Web user interface and configure the CT-5621T. To log on to the system from the Web browser, follow the steps below:

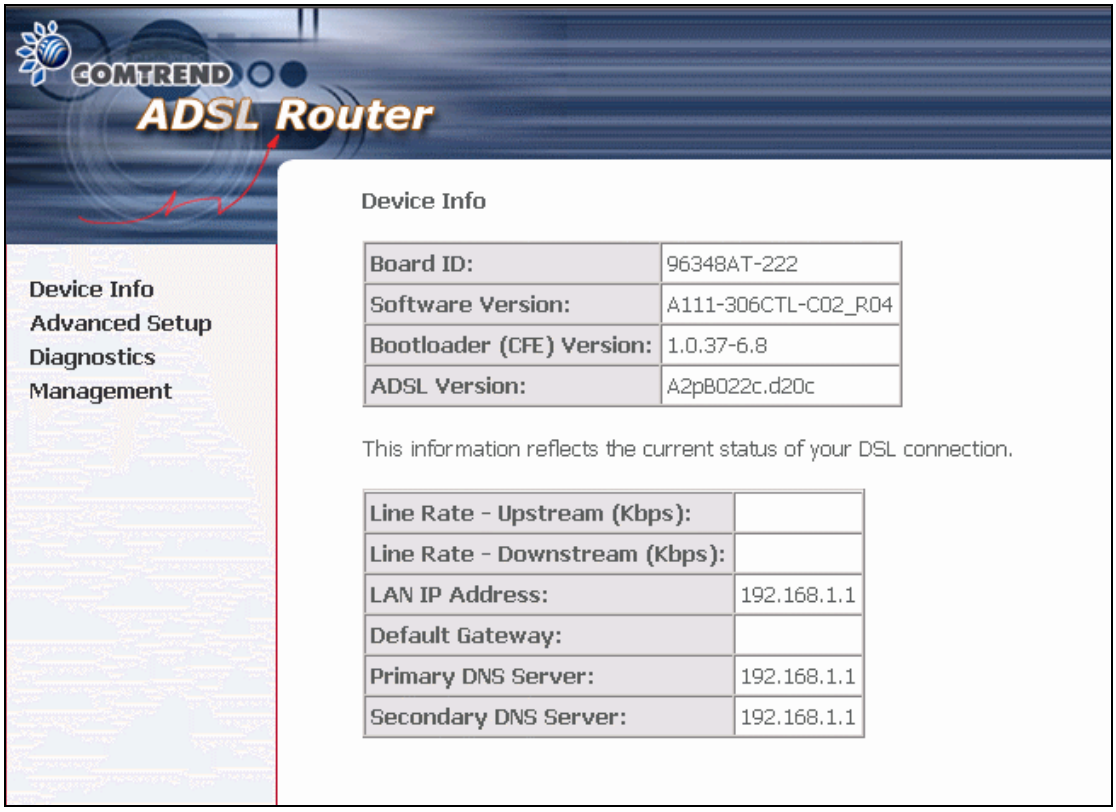
STEP 1: Start your Internet browser. Type the IP address for the router in the Web address field. For example, if the IP address is 192.168.1.1, type **http://192.168.1.1**

STEP 2: You will be prompted to enter your user name and password. Type **root** in the user name and **12345** in the password field, and click **OK**. These values can be changed later in the Web User Interface by selecting the **Management** link.



STEP 3: After successfully logging in, you will reach the Quick Setup menu.

Shown here is the **Device Info** screen for your reference.



3.3 Default Settings

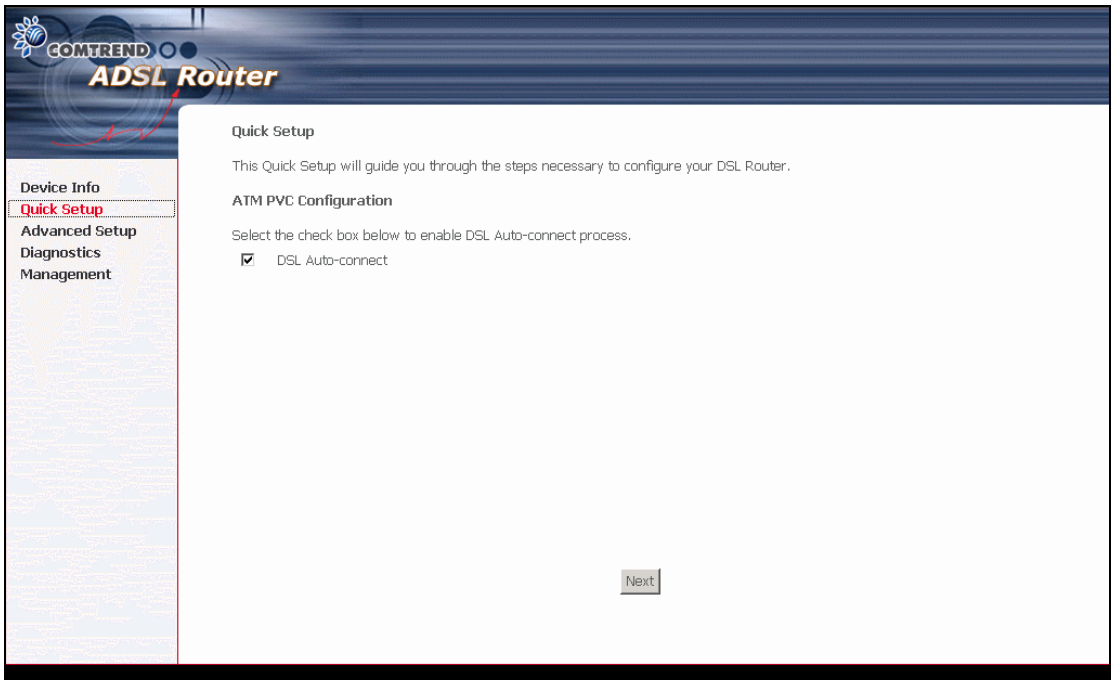
During power on initialization, the CT-5621T initializes all configuration attributes to default values. It will then read the configuration profile from the Permanent Storage section on the flash memory. The default attributes are overridden when identical attributes with different values are configured. The configuration profile in Permanent Storage can be created via the Web user interface, telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds, or by clicking the Restore Default Configuration option in the Restore Settings screen.

The following default settings are present when setting up the router for the first time. The PC running the browser can be attached to the Ethernet.

- LAN port IP address: 192.168.1.1
- Local administrator account name: root
- Local administrator account password: 12345
- Local non- administrator account name: user
- Local non- administrator account password: user
- Remote WAN access: disabled
- Remote WAN access account name: support
- Remote WAN access account password: support
- NAT and firewall: enabled
- DHCP server on LAN interface: enabled
- WAN IP address: none

Chapter 4 Device Info

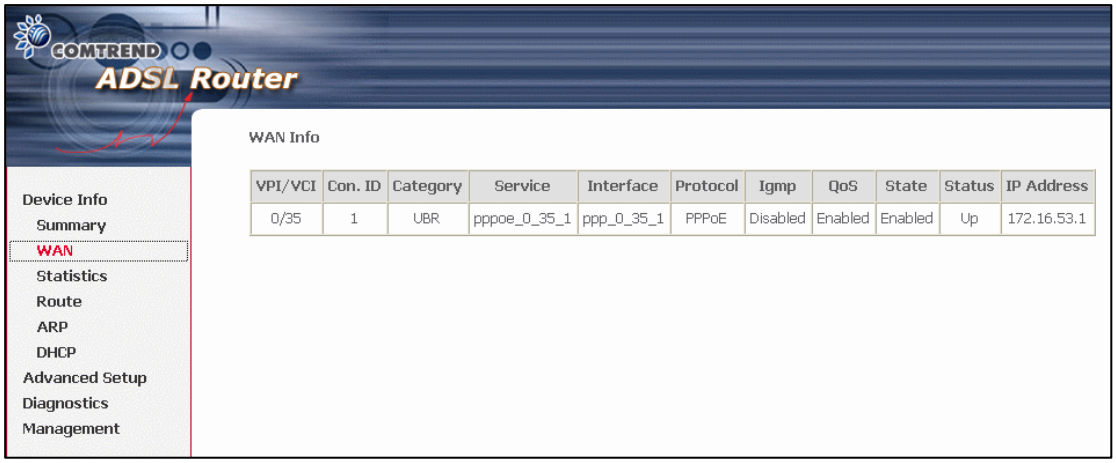
After login, the **Quick Setup** screen appears as shown.



Note: The selections available on the left side of menu are based upon the first configured connection and default user access settings.

4.1 WAN

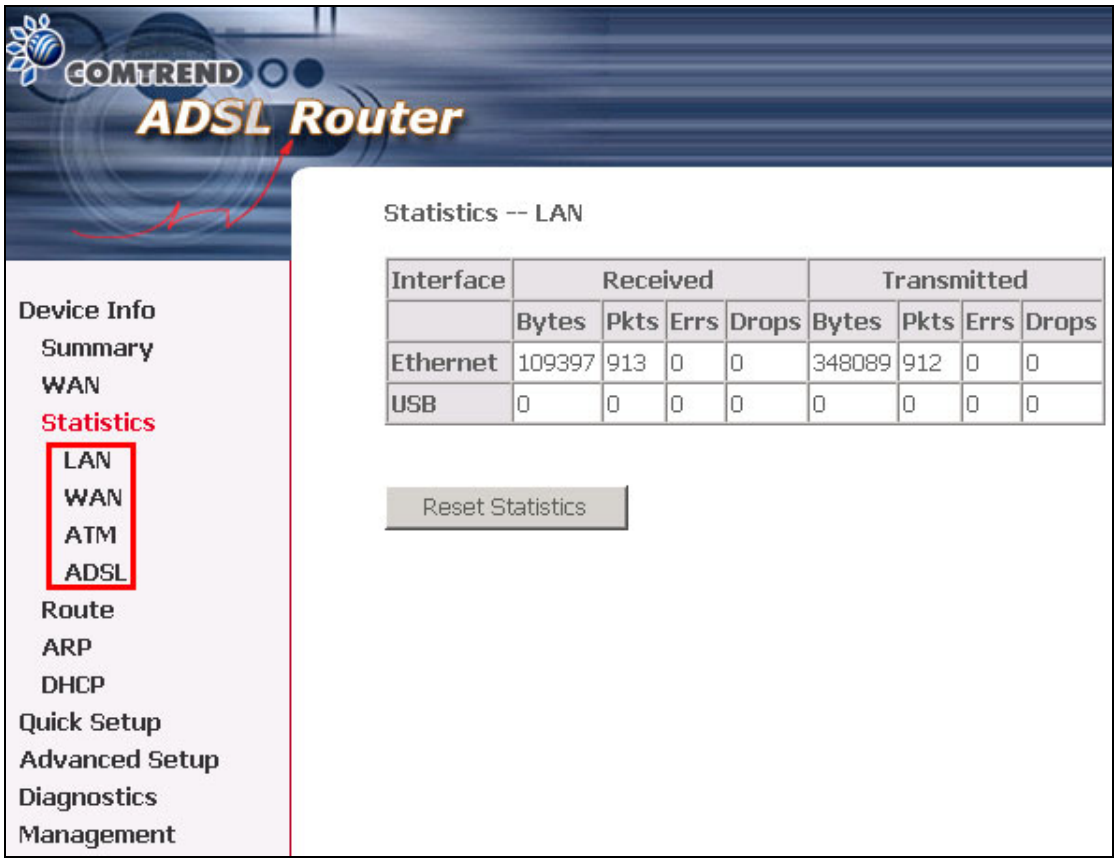
Click **Device Info** on the menu bar to display the WAN option. Then, click **WAN** on the Device Info menu bar to display the configured PVC(s) and the status.



VPI/VCI	Shows the values of the ATM VPI/VCI
Con. ID	Shows the connection ID
Category	Shows the ATM service classes
Service	Shows the name for WAN connection
Interface	Shows connection interfaces
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
IGMP	Shows the state of the IGMP function
Nat	Shows if the Network Address Translation (NAT) is enabled or disabled.
QoS	Shows if IGMP IP QoS is enabled or disabled
State	Shows the connection state of the WAN connection
Status	Lists the status of DSL link
IP Address	Shows IP address for WAN interface

4.2 Statistics

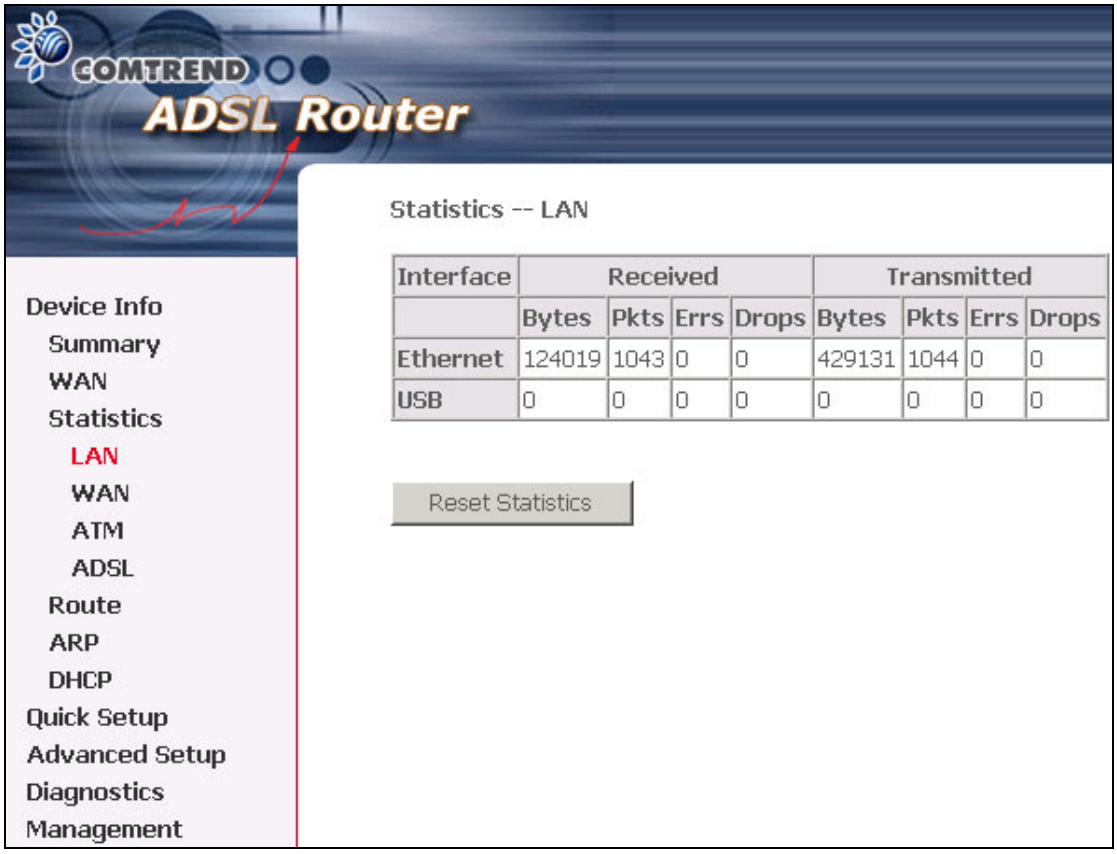
This menu option provides information on LAN, WAN, ATM and ADSL connections.



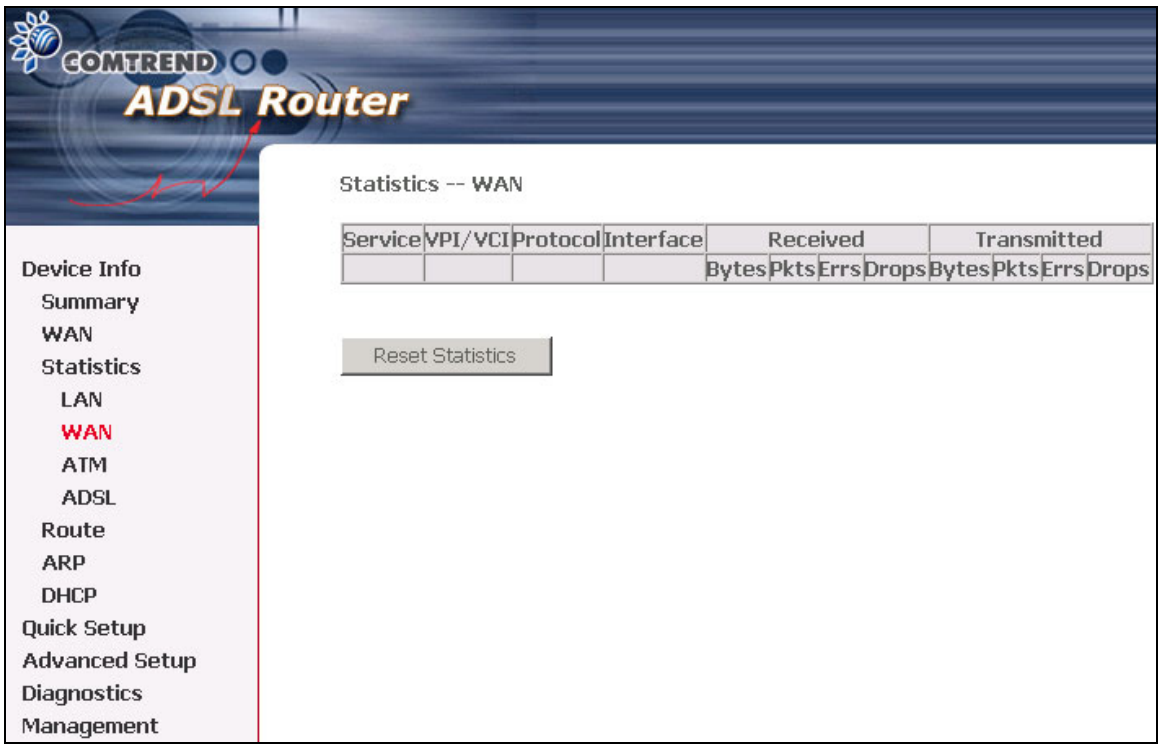
Note: These statistics are updated every 15 seconds.

4.2.1 LAN Statistics

The LAN Statistics screen shows byte transfer, packet transfer, Error and Drop statistics for each LAN interface (Ethernet and USB).



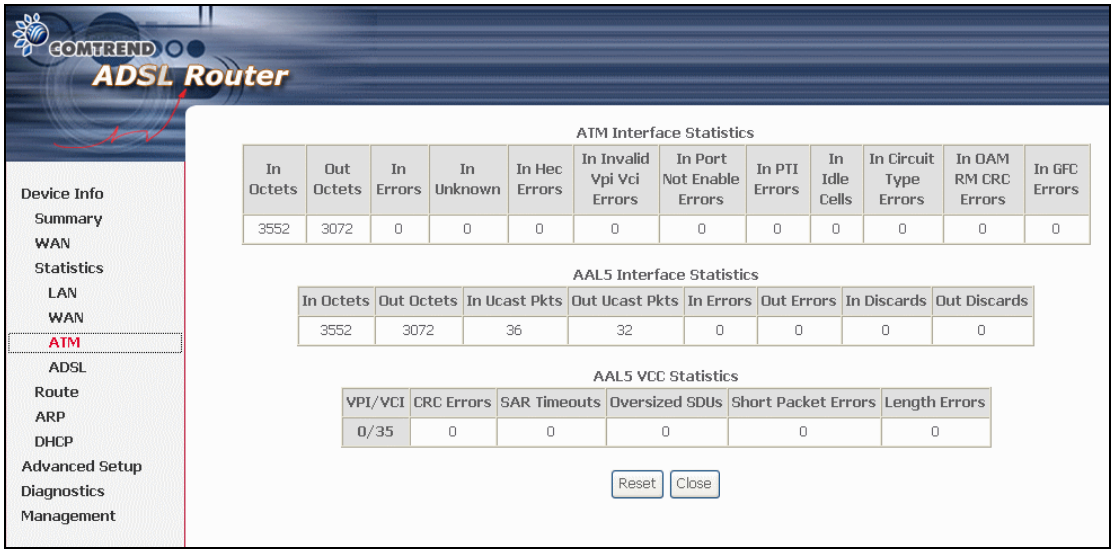
4.2.2 WAN Statistics



Service	Shows the service type
VPI/VCI	Shows the values of the ATM VPI/VCI
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
Interface	Shows connection interfaces
Received/Transmitted - Bytes - Pkts - Errs - Drops	 Number of Bytes Received/Transmitted Number of packets Received/Transmitted Number of errored packets Received/Transmitted Number of dropped packets Received/Transmitted

4.2.3 ATM statistics

The following figure shows the ATM statistics screen.


COMTREND
ADSL Router
Device Info
Summary
WAN
Statistics
LAN
WAN
ATM
ADSL
Route
ARP
DHCP
Advanced Setup
Diagnostics
Management
ATM Interface Statistics
In Octets | Out Octets | In Errors | In Unknown | In Hec Errors | In Invalid Vpi Vci Errors | In Port Not Enable Errors | In PTI Errors | In Idle Cells | In Circuit Type Errors | In OAM RM CRC Errors | In GFC Errors
3552 | 3072 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
AAL5 Interface Statistics
In Octets | Out Octets | In Ucast Pkts | Out Ucast Pkts | In Errors | Out Errors | In Discards | Out Discards
3552 | 3072 | 36 | 32 | 0 | 0 | 0 | 0
AAL5 VCC Statistics
VPI/VCI | CRC Errors | SAR Timeouts | Oversized SDUs | Short Packet Errors | Length Errors
0/35 | 0 | 0 | 0 | 0 | 0
Reset
Close

ATM Interface Statistics

Field	Description
In Octets	Number of received octets over the interface
Out Octets	Number of transmitted octets over the interface
In Errors	Number of cells dropped due to uncorrectable HEC errors
In Unknown	Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here.
In Hec Errors	Number of cells received with an ATM Cell Header HEC error
In Invalid Vpi Vci Errors	Number of cells received with an unregistered VCC address
In Port Not Enable Errors	Number of cells received on a port that has not been enabled
In PTI Errors	Number of cells received with an ATM header Payload Type Indicator (PTI) error
In Idle Cells	Number of idle cells received
In Circuit Type Errors	Number of cells received with an illegal circuit type

In Oam RM CRC Errors	Number of OAM and RM cells received with CRC errors
In GFC Errors	Number of cells received with a non-zero GFC

AAL5 Interface Statistics

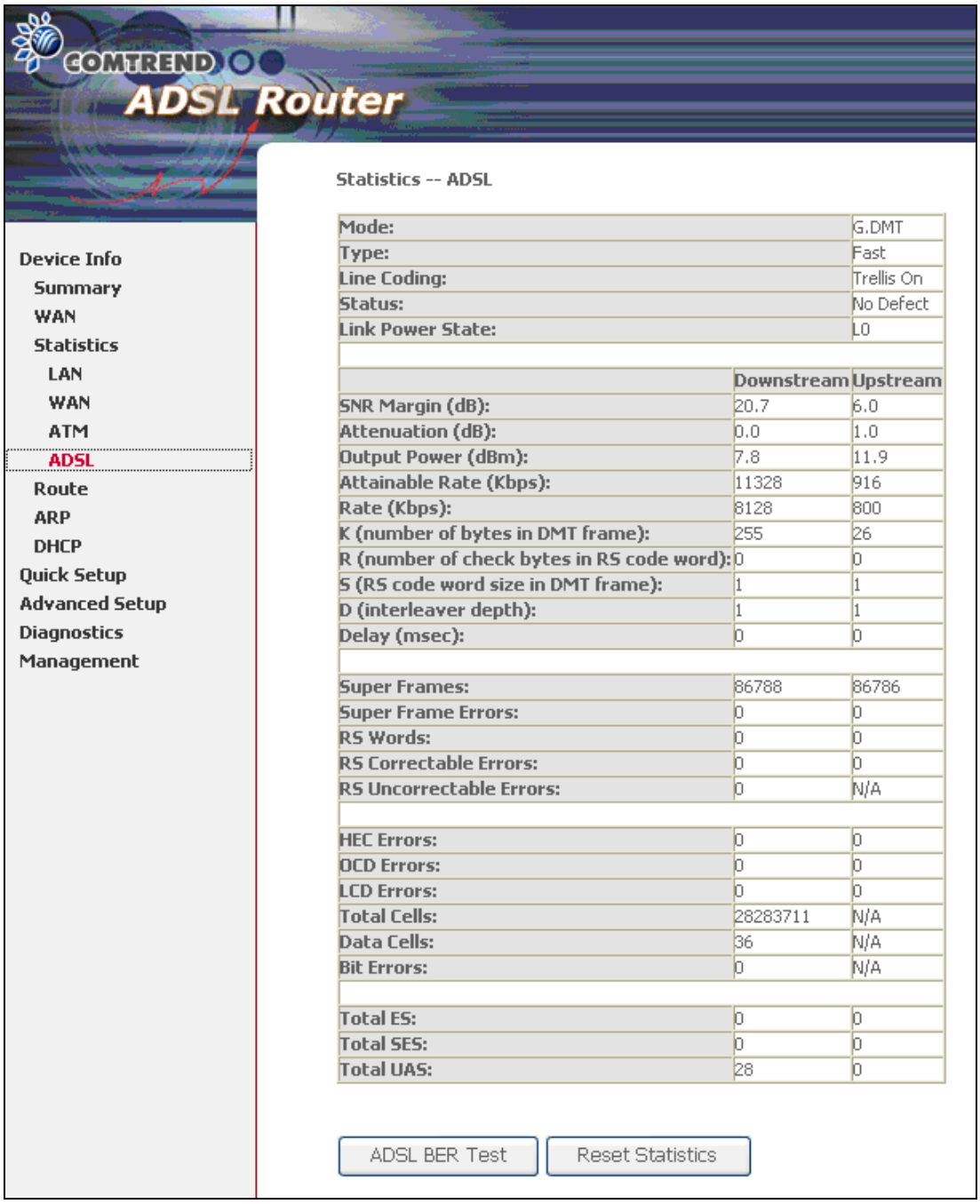
Field	**Description**
In Octets	Number of received AAL5/AAL0 CPCS PDU octets
Out Octets	Number of AAL5/AAL0 CPCS PDU octets transmitted
In Ucast Pkts	Number of received AAL5/AAL0 CPCS PDU passed to a higher-layer
Out Ucast Pkts	Number of received AAL5/AAL0 CPCS PDU received from a higher layer for transmission
In Errors	Number of received AAL5/AAL0 CPCS PDU in error. The types of errors counted include CRC-32 errors.
Out Errors	Number of received AAL5/AAL0 CPCS PDU that could not be transmitted due to errors.
In Discards	Number of received AAL5/AAL0 CPCS PDU discarded due to an input buffer overflow condition.
Out Discards	This field is not currently used

AAL5 VCC STATISTICS

Field	**Description**
VPI/VCI	Shows the values of the ATM VPI/VCI
CRC Errors	Number of PDUs received with CRC-32 errors
SAR TimeOuts	Number of partially re-assembled PDUs which were discarded because they were not fully re-assembled within the required period of time. If the re-assembly time is not supported then, this object contains a zero value.
Over Sized SDUs	Number of PDUs discarded because the corresponding SDU was too large
Short Packets Errors	Number of PDUs discarded because the PDU length was less than the size of the AAL5 trailer
Length Errors	Number of PDUs discarded because the PDU length did not match the length in the AAL5 trailer

4.2.4 ADSL Statistics

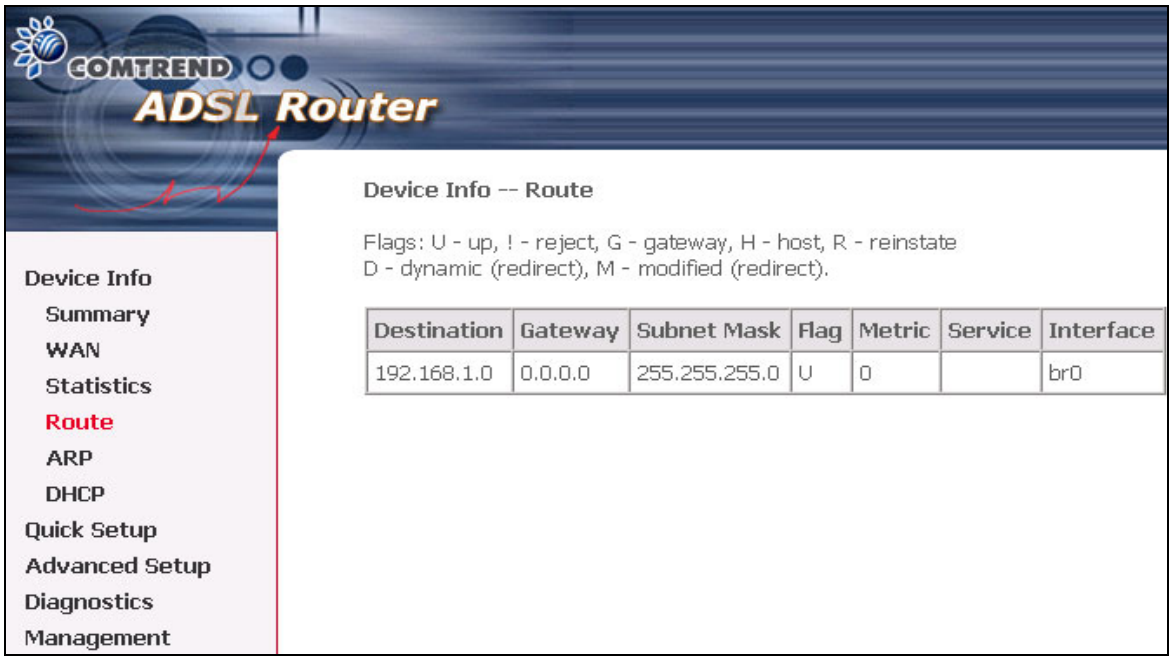
The following figure shows the ADSL Network Statistics screen. Within the ADSL Statistics window, a bit Error Rate Test can be started using the ADSL BER Test button. The Reset button resets the statistics.



Field	Description
Mode	Line Coding format, that can be selected G.dmt, G.lite, T1.413, ADSL2
Type	Channel type Interleave or Fast
Line Coding	Trellis On/Off
Status	Lists the status of the DSL link
Link Power State	Link output power state.
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.
Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of out-of-cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

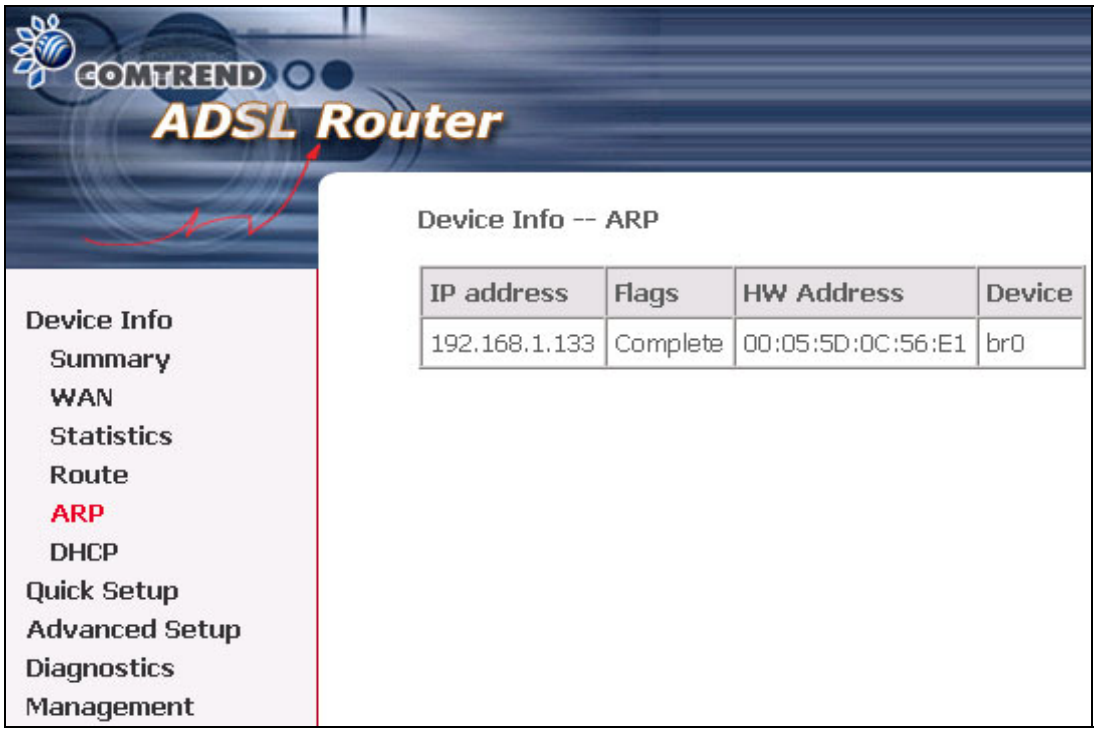
4.2.5 Route

Choose **Route** to display the routes that the route information has learned.



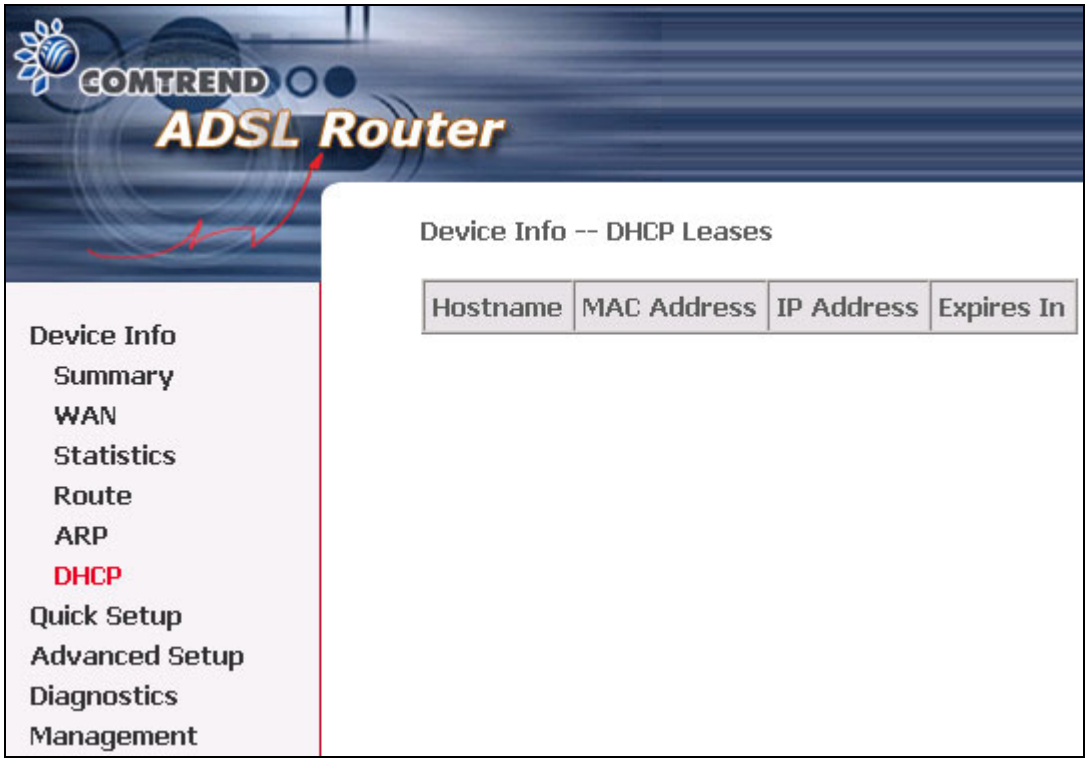
4.2.6 ARP

Click **ARP** to display the ARP information.



4.2.7 DHCP

Click **DHCP** to display the DHCP information.



Chapter 5 Quick Setup

The Quick Setup allows the user to configure the ADSL router for DSL connectivity and Internet access. It also guides the user though the WAN network setup first and then the LAN interface setup. You can either manually customize the router or follow the online instruction to set up the router.

The CT-5621T ADSL router supports the following five network operating modes over an ATM PVC WAN interface.

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoA)
- MAC Encapsulated Routing (MER)
- IP over ATM (IPoA)
- Bridging

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration on the Central Office side and Broadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the CT-5621T is to run the PPPoE client. The CT-5621T can support both cases simultaneously.
- If some or none of the LAN-side devices do not run PPPoE client, then select PPPoE. If every LAN-side device is running a PPPoE client, then select Bridge In PPPoE mode, CT-5621T also supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client fro non-PPPoE LAN devices. NAT and firewall are always enabled when PPPoE mode is selected, but they can be enabled or disabled by the user when MER or IPoA is selected, NAT and firewall are always disabled when Bridge mode is selected.
- Depending on the network operating mode, and whether NAPT and firewall are enabled or disabled, the main panel will display or hide the NAPT/Firewall menu. For instance, at initial setup, the default network operating mode is Bridge. The main panel will not show the NAPT and Firewall menu.

Note: Up to sixteen PVC profiles can be configured and saved on the flash memory. To activate a particular PVC profile, you need to navigate all the Quick Setup pages until the last summary page, then click on the Finish button and reboot the system.

5.1 Auto Quick Setup

The auto quick setup requires the ADSL link to be up. The ADSL router will automatically detect the PVC. You only need to follow the online instructions that you are prompted.

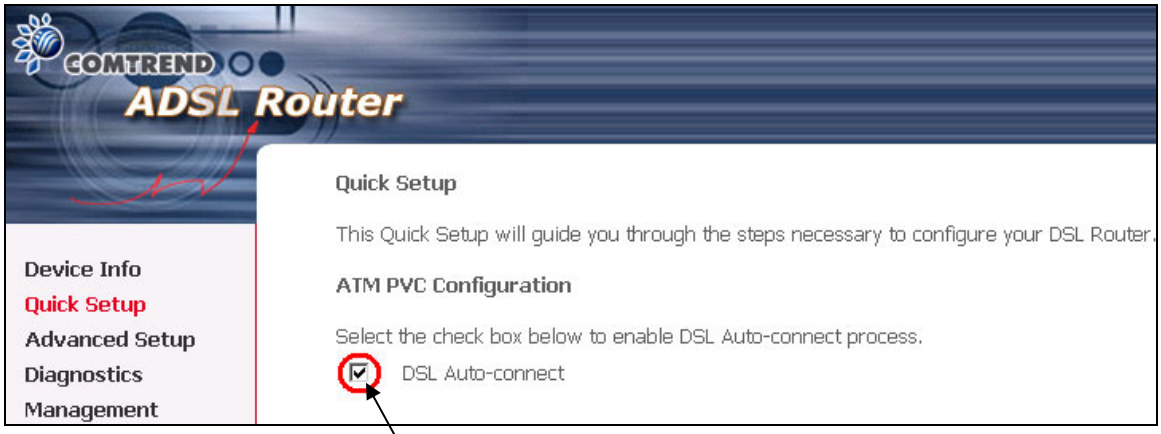
1. Select **Quick Setup** to display the DSL Quick Setup screen.

2. Click **Next** to start the setup process. Follow the online instructions to complete the setting. This procedure will skip some processes like PVC index, or encapsulation.

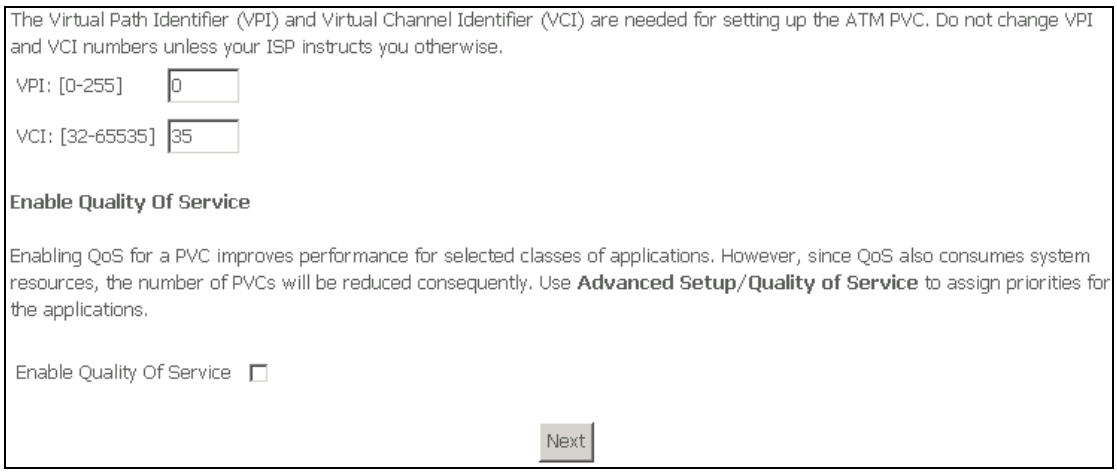
3. After the settings are complete, you can use the ADSL service.

5.2 Manual Quick Setup

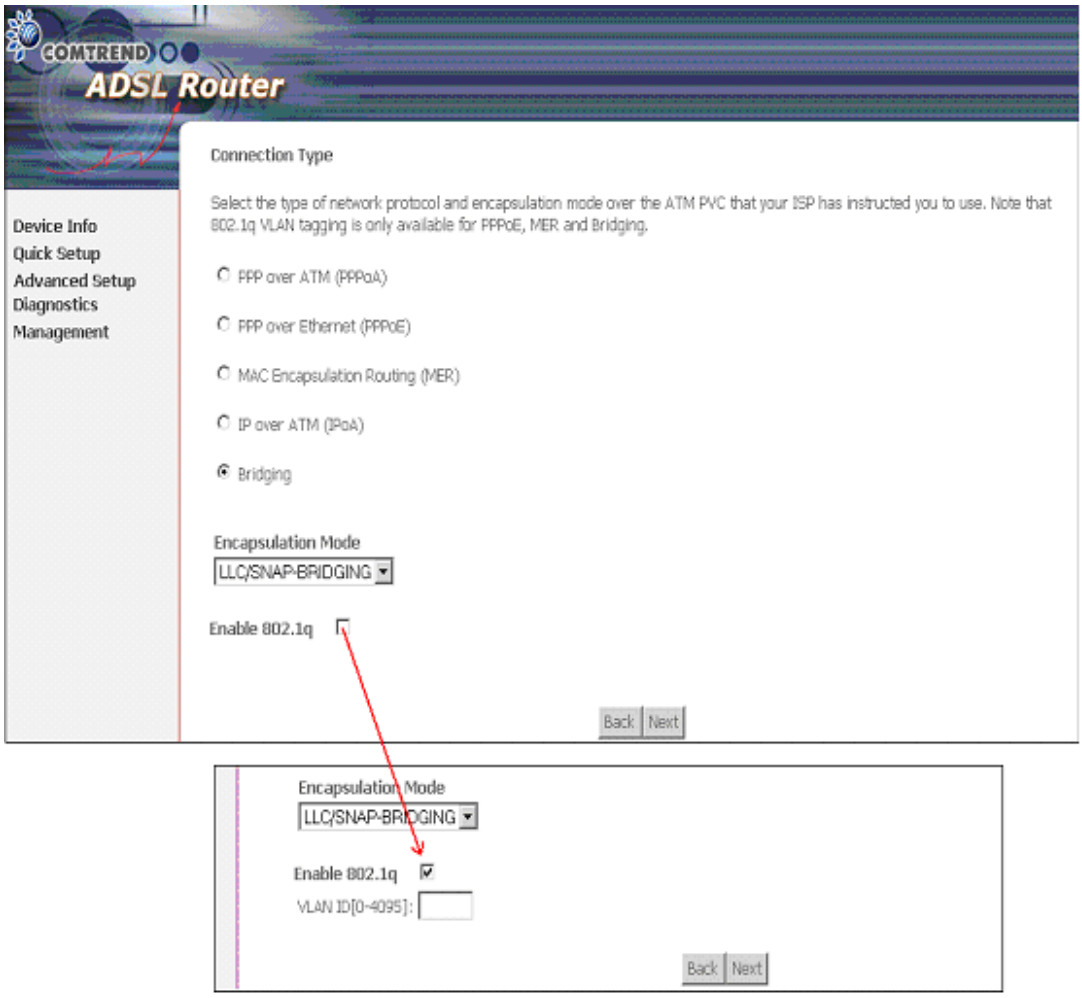
STEP 1: Click **Quick Setup** and un-tick the **DSL Auto-connect** checkbox to enable manual configuration of the connection type.



Un-tick this checkbox to enable manual setup and display the following screen.


The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.
VPI: [0-255] 0
VCI: [32-65535] 35
Enable Quality Of Service
Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service
Next

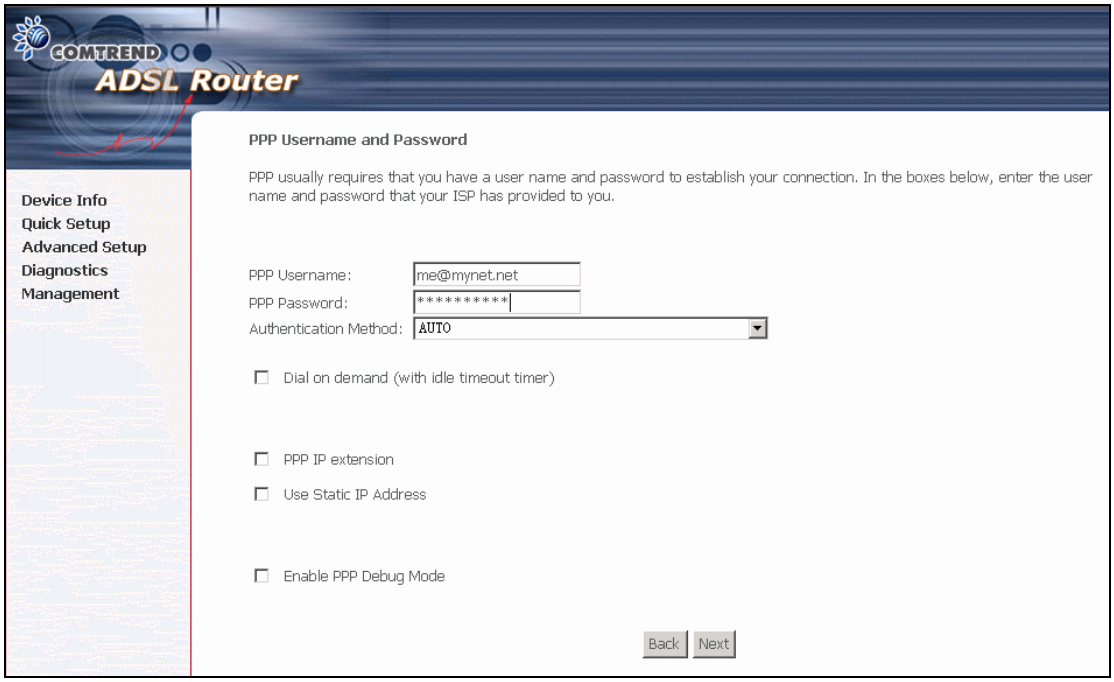
STEP 2: Enter the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). Select Enable Quality Of Service if required. Click **Next**.



STEP 3: Choosing different connection types pops up different settings requests. Enter appropriate settings that are requested by your service provider. The following descriptions state each connection type setup separately. Select **Enable 802.1q** (by ticking the box) if required, and input a number for the VLAN ID. Click on "Next" to go to next step.

5.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)

1. Select the **PPP over ATM (PPPoA)** or **PPP over Ethernet (PPPoE)** radio button and click **Next**. The following screen appears:



PPP USERNAME/PPP PASSWORD

Give "PPP Username", "PPP Password" and "PPPoE Service Name", and then select the "Authentication Method" (AUTO/PAP/CHAP/MSCHAP). Please contact your ISP for the information. The WEB user interface allows a maximum of 256 characters in the PPP user name and a maximum of 32 characters in PPP password.

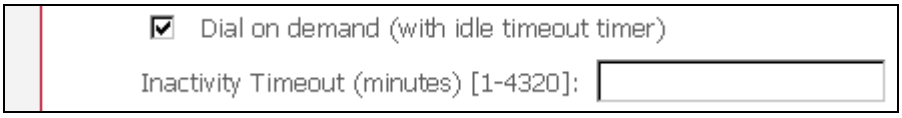
Encapsulation Mode

Choosing different connection types provides different encapsulation modes.

- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP BRIDGING, VC/MUX
- MER- LLC/SNAP-BRIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC MUX
- Bridging- LLC/SNAP-BRIDGING, VC/MUX

Disconnect if no activity

The CT-5621T can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** check box. When the checkbox is ticked, you need to enter the inactivity timeout period. The timeout period ranges from 1 minute to 4320 minutes.



PPP IP Extension

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specially requires this setup, do not select it.

The PPP IP Extension supports the following conditions:

- Allows only one PC on the LAN
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the ADSL router has a single IP address to assign to a LAN device.
- NAPT and firewall are disabled when this option is selected.
- The ADSL router becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The ADSL router extends the IP subnet at the remote service provider to the LAN PC. That is, the PC becomes a host belonging to the same IP subnet.
- The ADSL router bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the router's LAN IP address.

Use Static IP Address

Unless your service provider specially requires this setup, do not select it.

If selected, enter your static IP address.

Enable PPP Debug Mode

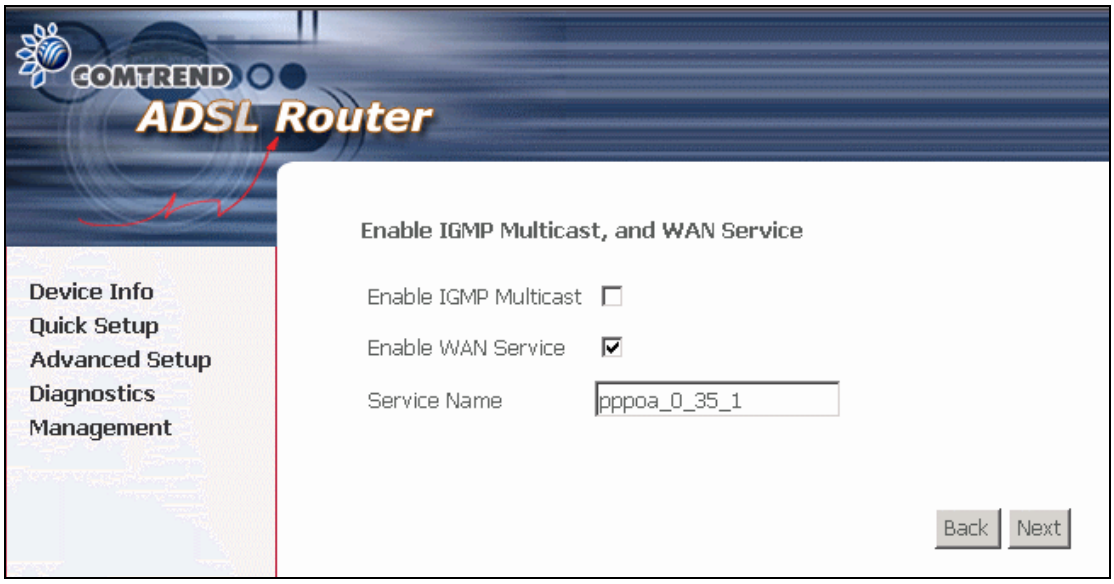
Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. But this is for debug, please don't enable in normal usage.

2. Click **Next** to display the screen on the following page.

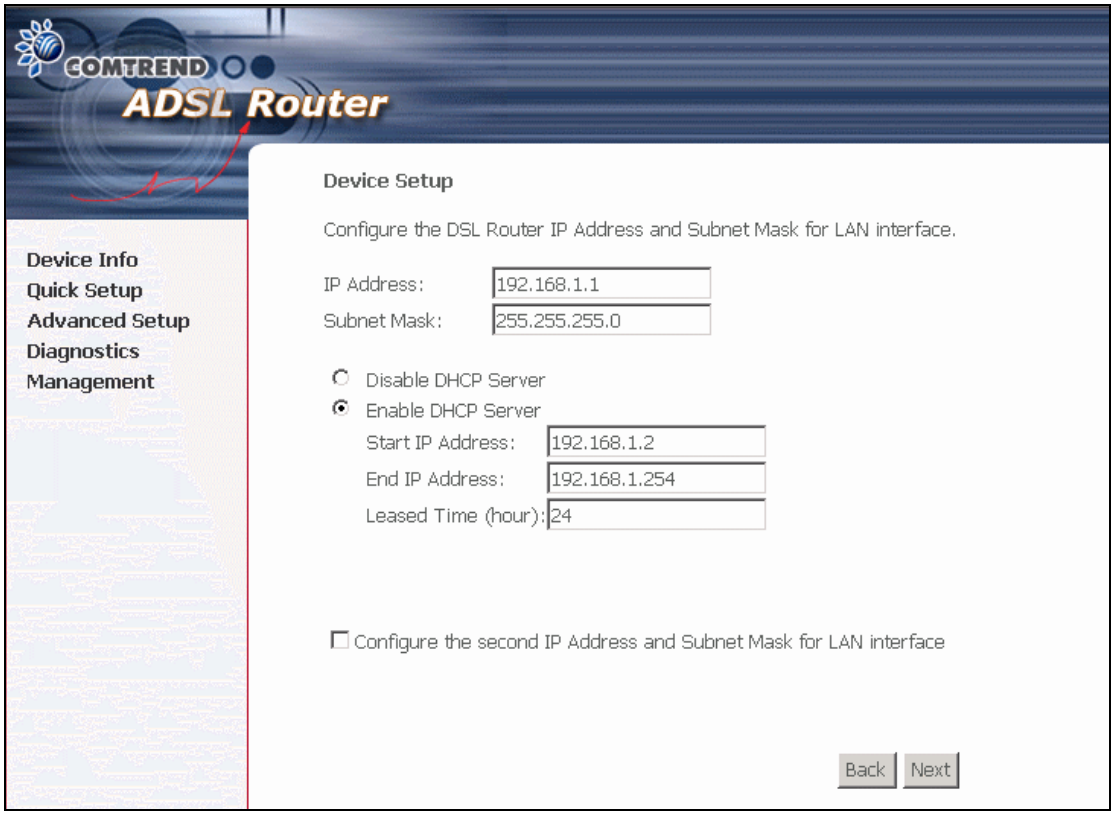
Enable IGMP Multicast checkbox: Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service checkbox: Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is user-defined.



3. After entering your settings, select **Next**. The following screen appears. This page allows the user to configure the LAN interface IP address, subnet mask and DHCP server. If the user would like this ADSL router to assign dynamic IP address, DNS server and default gateways to other LAN devices, select the button **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP leased time.



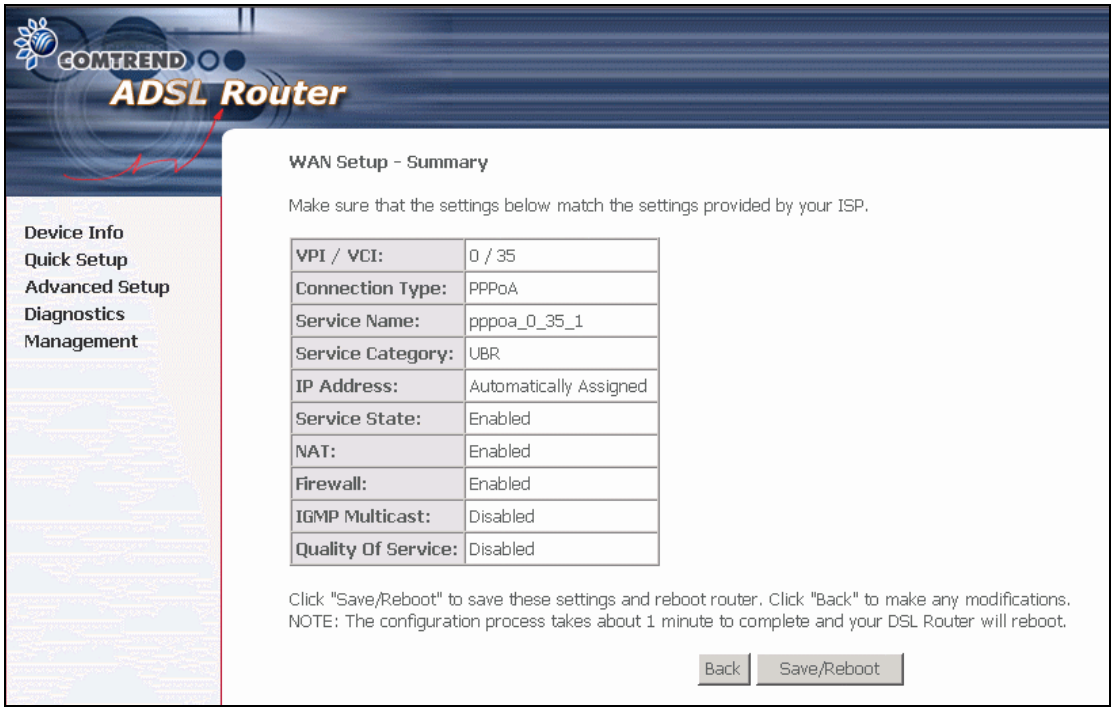
The Device Setup page allows the user to configure the LAN interface IP address and DHCP server. If the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Note 1: Enable DHCP Server Relay will not display if Firewall is enabled in the previous step.

Note 2: The router's default IP address is 192.168.1.1 and the default private address range provided by the ISP server in the router is 192.168.1.2 through 192.168.1.254.

4. Click **Next** to display the WAN Setup-Summary screen that presents the entire configuration summary.

- Click **Save/Reboot** if the settings are correct.
- Click **Back** if you wish to modify the settings.

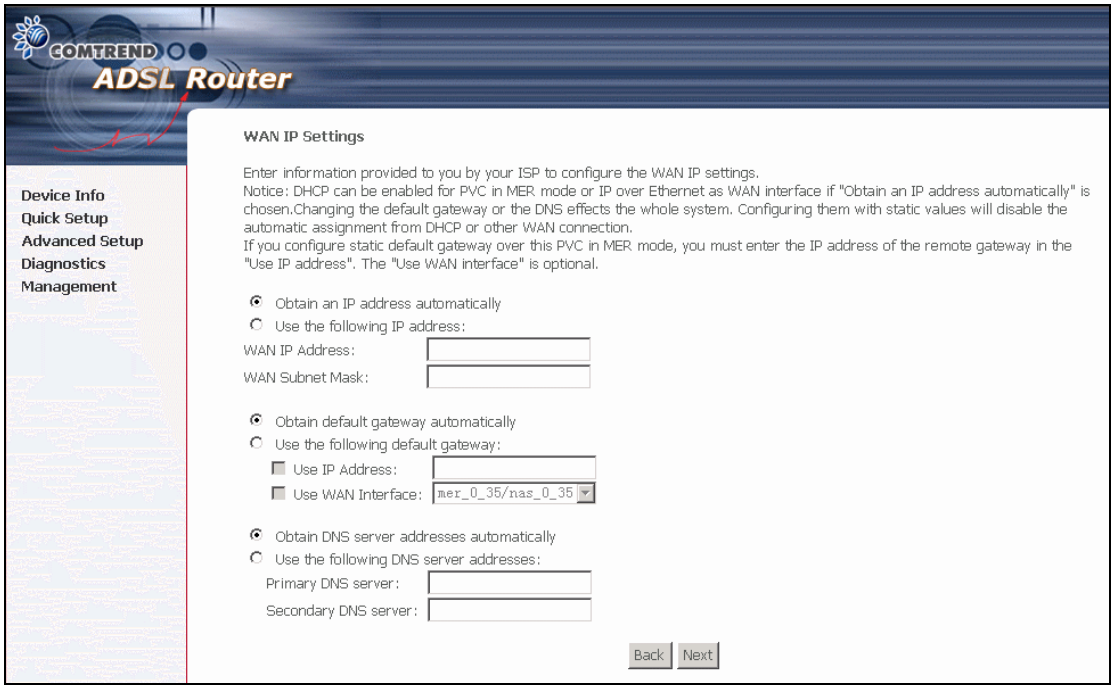

COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 0 / 35
Connection Type: PPPoA
Service Name: pppoa_0_35_1
Service Category: UBR
IP Address: Automatically Assigned
Service State: Enabled
NAT: Enabled
Firewall: Enabled
IGMP Multicast: Disabled
Quality Of Service: Disabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

5. After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-5621T is ready for operation and the front panel LED indicators will display as described in section 1.3.

5.2.2 MAC Encapsulation Routing (MER)

To configure MER, do the following.

1. Select **Quick Setup** and click **Next**.
2. Enter the PVC Index provided by the ISP and click **Next.**
3. Select the MAC Encapsulation Routing (MER) radio button, and click **Next**. The following screen appears.


COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management
WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen.Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.
Obtain an IP address automatically
Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
Obtain default gateway automatically
Use the following default gateway:
Use IP Address:
Use WAN Interface:
mer_0_35/nas_0_35
Obtain DNS server addresses automatically
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

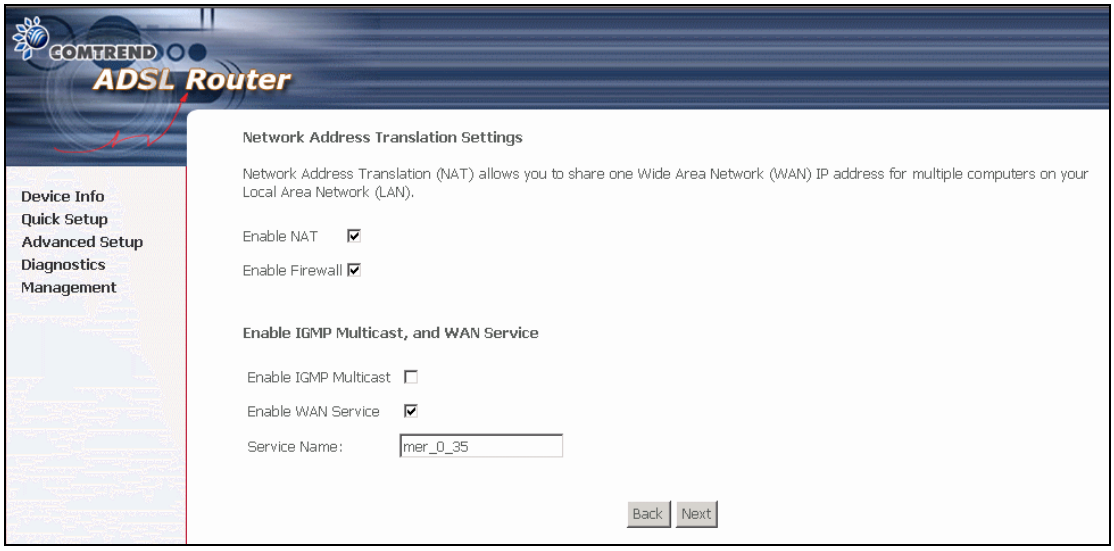
Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: DHCP can be enabled for PVC in MER mode if **Obtain an IP address automatically** is chosen. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.

If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

The ISP should provide the values that must be entered in the entry fields.

4. Click Next to display the following screen.



Enable NAT checkbox: If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel.

Enable Firewall checkbox: If the firewall checkbox is selected, the Security submenu on the left side main panel will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will not be displayed on the left main panel.

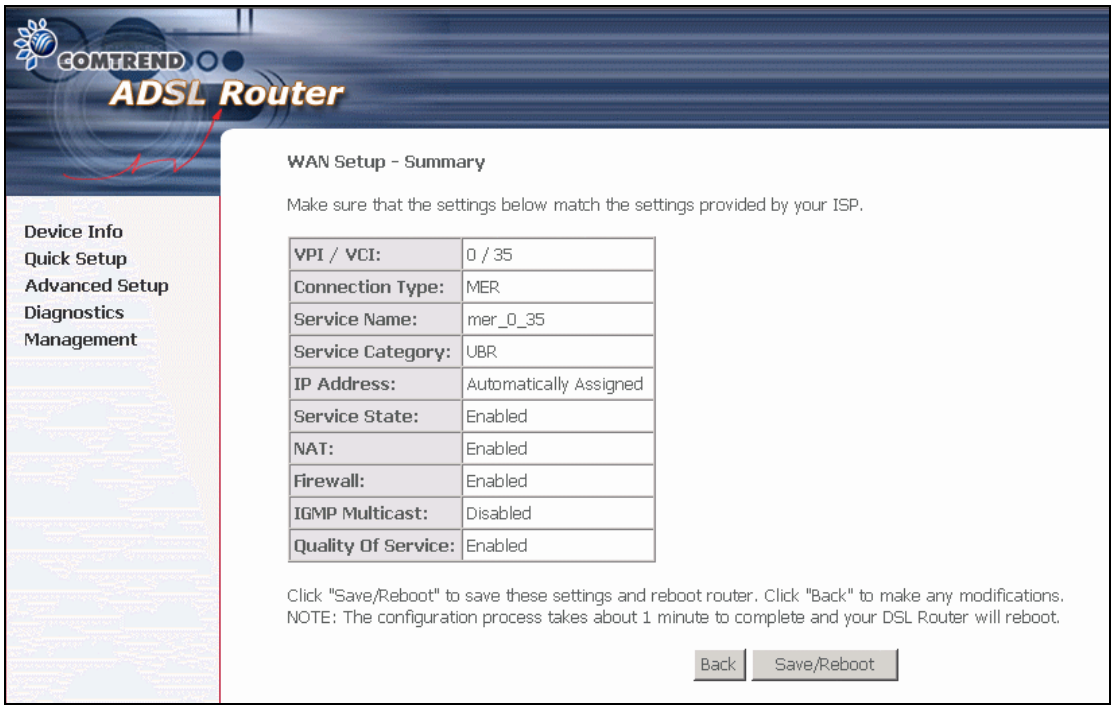
Enable IGMP Multicast: Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service: Tick the checkbox to enable the WAN service. If this item is not selected, you will not be able to use the WAN service.

Service Name: This is User-defined.

5. Upon completion, click **Next**. The following screen appears. The **WAN Setup-Summary** screen presents the entire configuration summary.

   - Click **Save/Reboot** if the settings are correct.
   - Click **Back** if you wish to modify the settings.

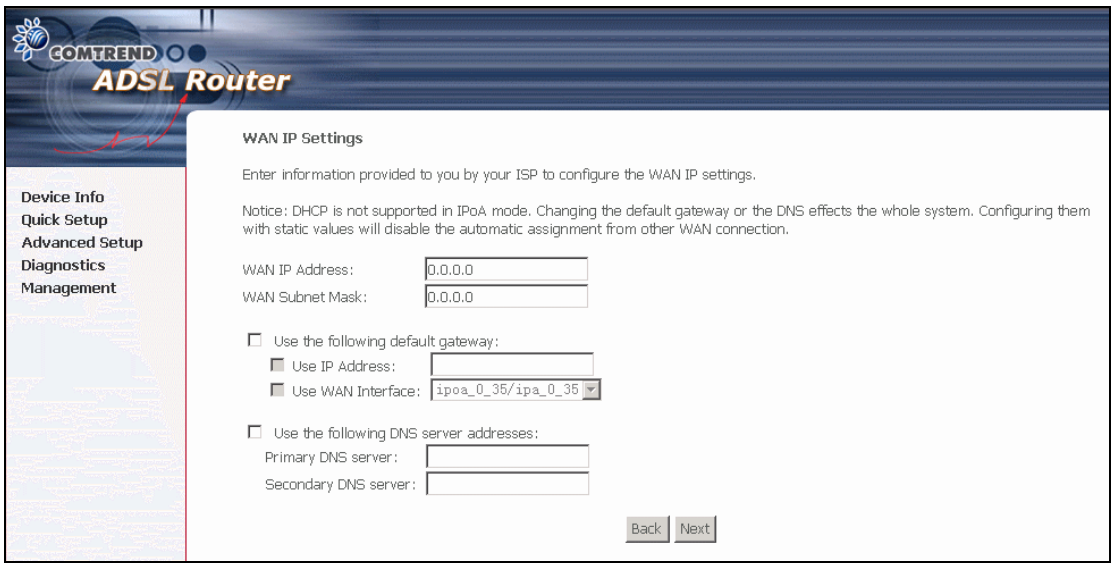

COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 0 / 35
Connection Type: MER
Service Name: mer_0_35
Service Category: UBR
IP Address: Automatically Assigned
Service State: Enabled
NAT: Enabled
Firewall: Enabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-5621T is ready for operation and the front panel LED indicators will display as described in section 1.3.

5.2.3 IP Over ATM

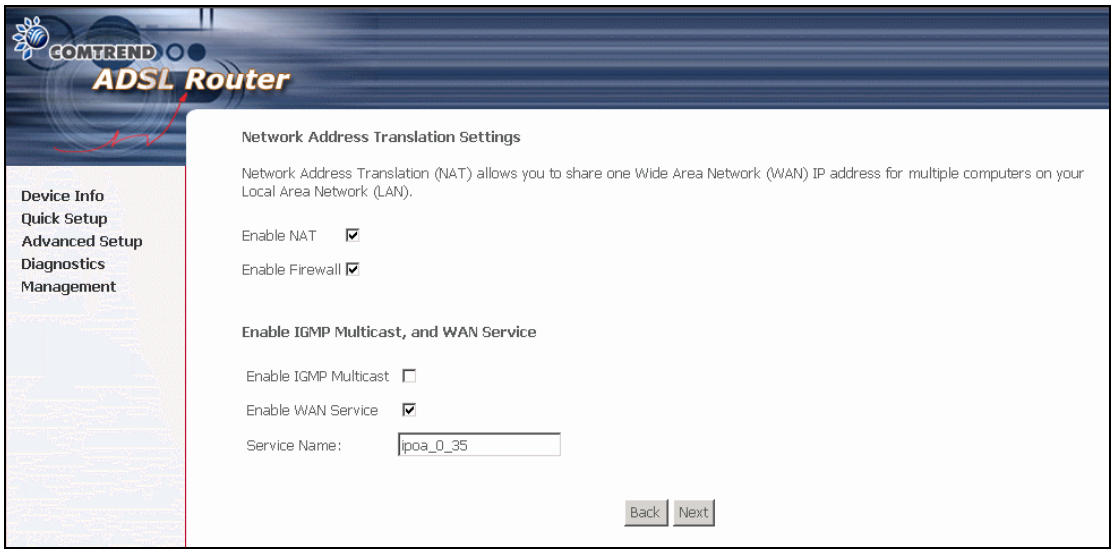
To configure IP Over ATM,

1. Select **Quick Setup** and click **Next**.
2. Enter the PVC Index and click **Next**.
3. Type the VPI and VCI values provided by the ISP and click **Next**.
4. Select the IP over ATM (IPoA) radio button and click **Next**.
   The following screen will appear.


COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management
WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection.
WAN IP Address: 0.0.0.0
WAN Subnet Mask: 0.0.0.0
Use the following default gateway:
Use IP Address:
Use WAN Interface: ipoa_0_35/ipa_0_35
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

Notice that DHCP is not supported over IPoA. The user must enter the IP address or WAN interface for the default gateway setup, and the DNS server addresses provided by the ISP.

5. Click **Next**. The following screen appears.



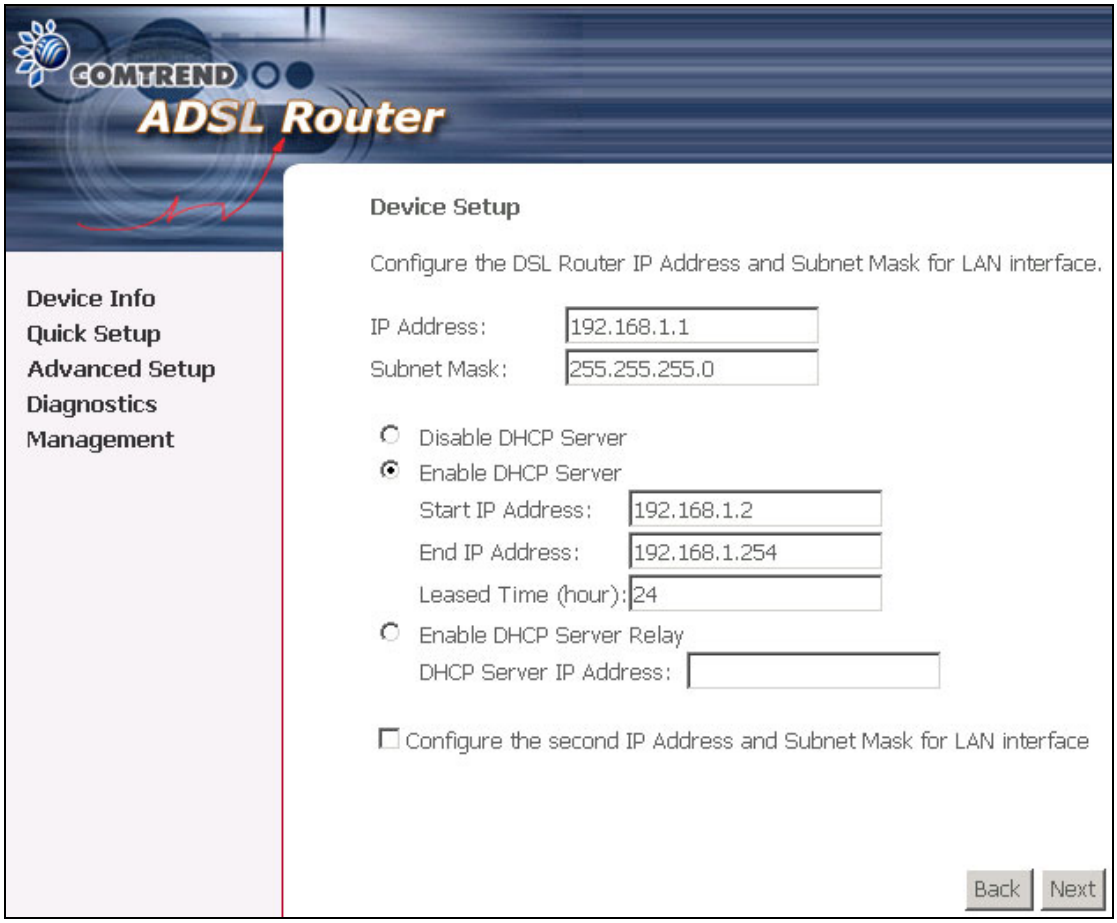
Enable NAT checkbox

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox should be de-selected. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel.

Enable Firewall checkbox

If the firewall checkbox is selected, the Security submenu on the left side main panel will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will not be displayed on the left main panel.

6. Click **Next** to display the following screen. The Device Setup page allows the user to configure the LAN interface IP address and DHCP server if the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices. Select the button Enable DHCP server on the LAN to enter the starting IP address and end IP address and DHCP lease time.

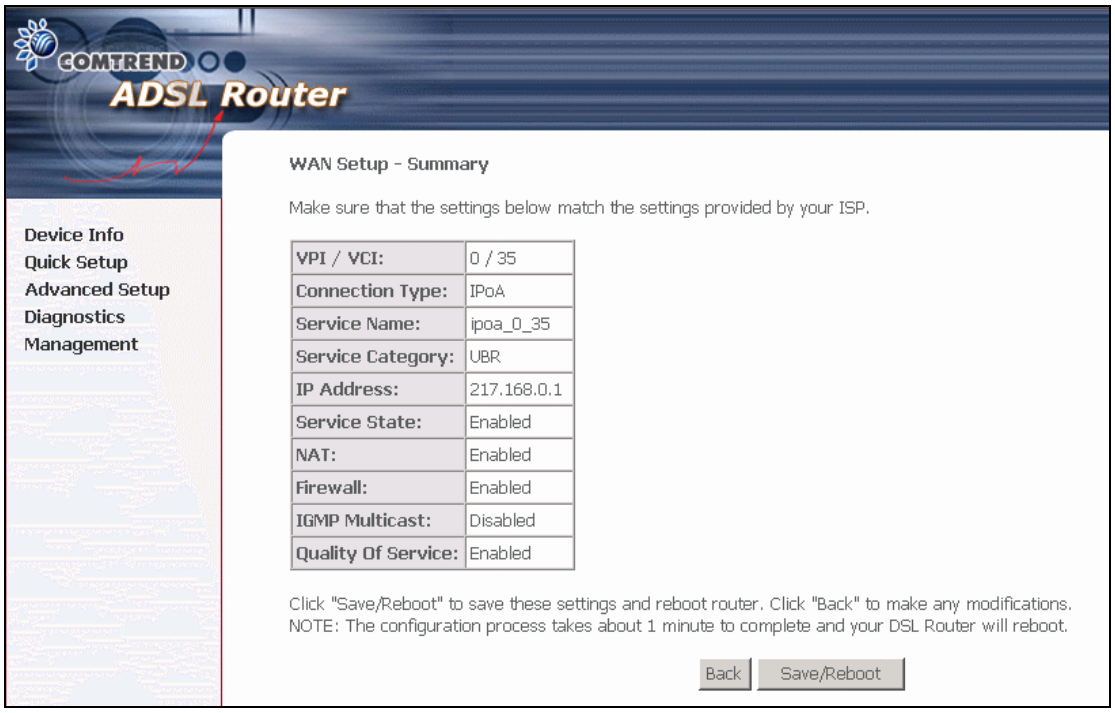


The user must configure the IP Address and the Subnet Mask. To use the DHCP service on the LAN, select the **Enable DHCP server** checkbox, and enter the Start IP addresses, the End IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Note 1: Enable DHCP Server Relay will not display if Firewall is enabled in the previous step.

Note 2: The router's default IP address is 192.168.1.1 and the default private address range provided by the ISP server in the router is 192.168.1.2 through 192.168.1.254.

7. Click the **Next** button to continue. The following screen will be displayed.

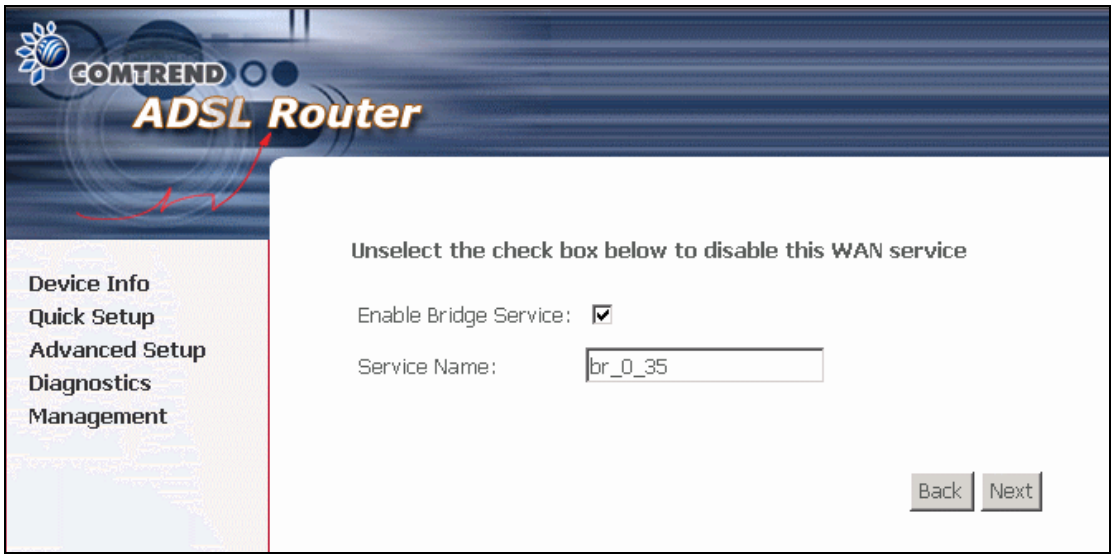

COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 0 / 35
Connection Type: IPoA
Service Name: ipoa_0_35
Service Category: UBR
IP Address: 217.168.0.1
Service State: Enabled
NAT: Enabled
Firewall: Enabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

8. After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-5621T is ready for operation and the front panel LED indicators will display as described in section 1.3.

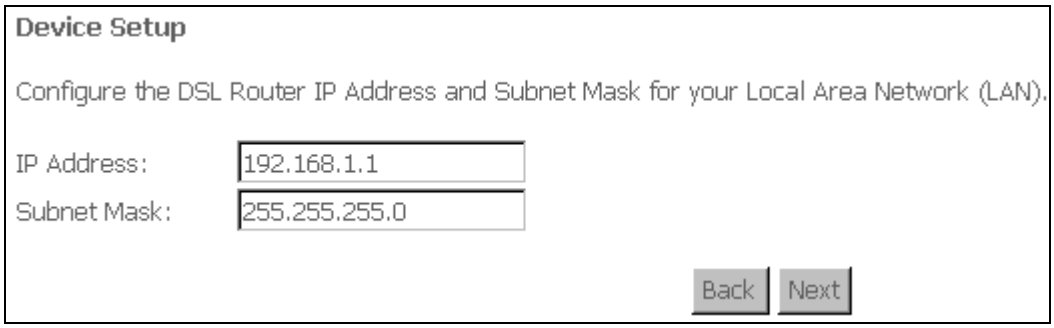
5.2.4 Bridging

Select the bridging mode. To configure Bridging, do the following.

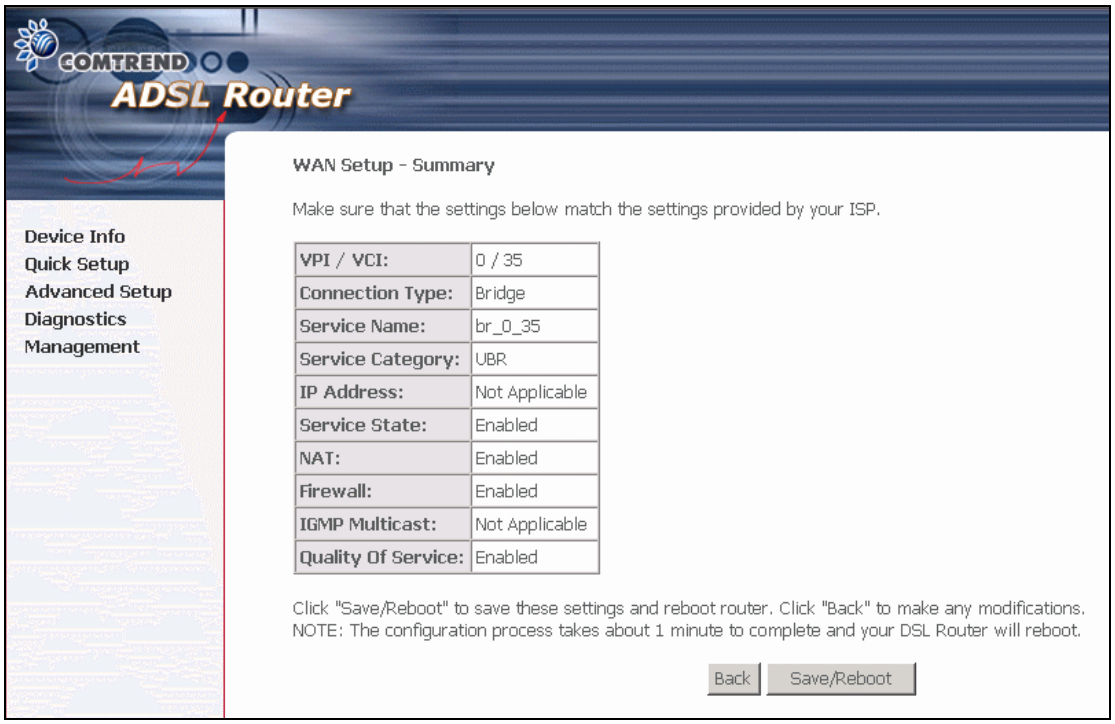
1. Select Quick Setup and click **Next**.
2. Enter the PVC Index and click **Next**.
3. Type in the VPI and VCI values provided by the ISP and click Next.
4. Select the Bridging radio button and click **Next**. The following screen appears. To use the bridge service, tick the checkbox, Enable Bridge Service, and enter the service name.



5. Click the **Next** button to continue. Enter the IP address for the LAN interface. The default IP address is 192.168.1.1. The LAN IP interface in bridge operating mode is needed for local users to manage the ADSL router. Notice that there is no IP address for the WAN interface in bridge mode, and the remote technical support cannot access the ADSL router.



6. Click the **Next** button to continue. The following screen will be displayed.

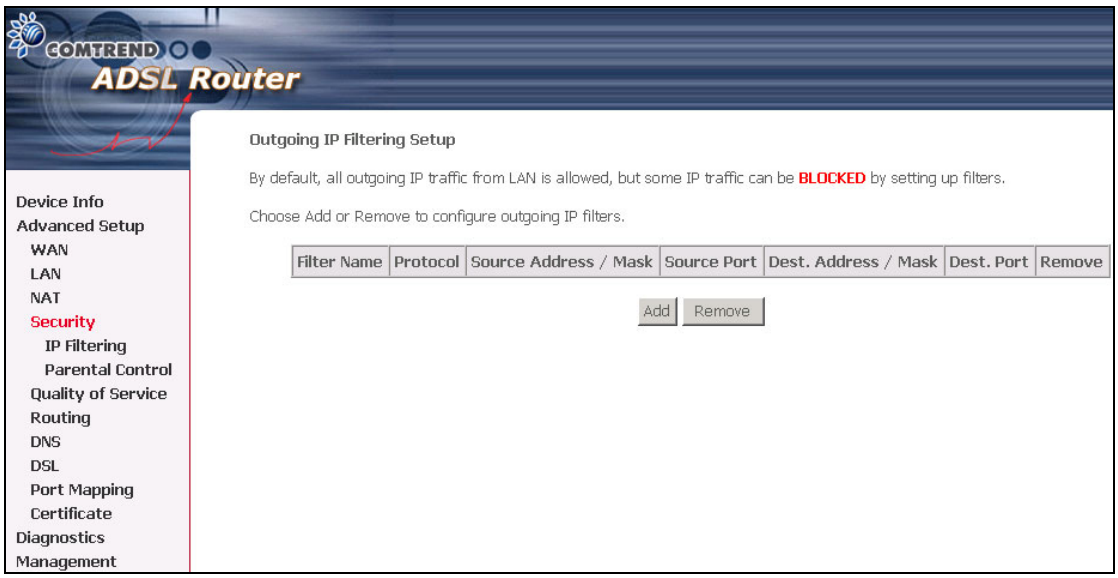

COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 0 / 35
Connection Type: Bridge
Service Name: br_0_35
Service Category: UBR
IP Address: Not Applicable
Service State: Enabled
NAT: Enabled
Firewall: Enabled
IGMP Multicast: Not Applicable
Quality Of Service: Enabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

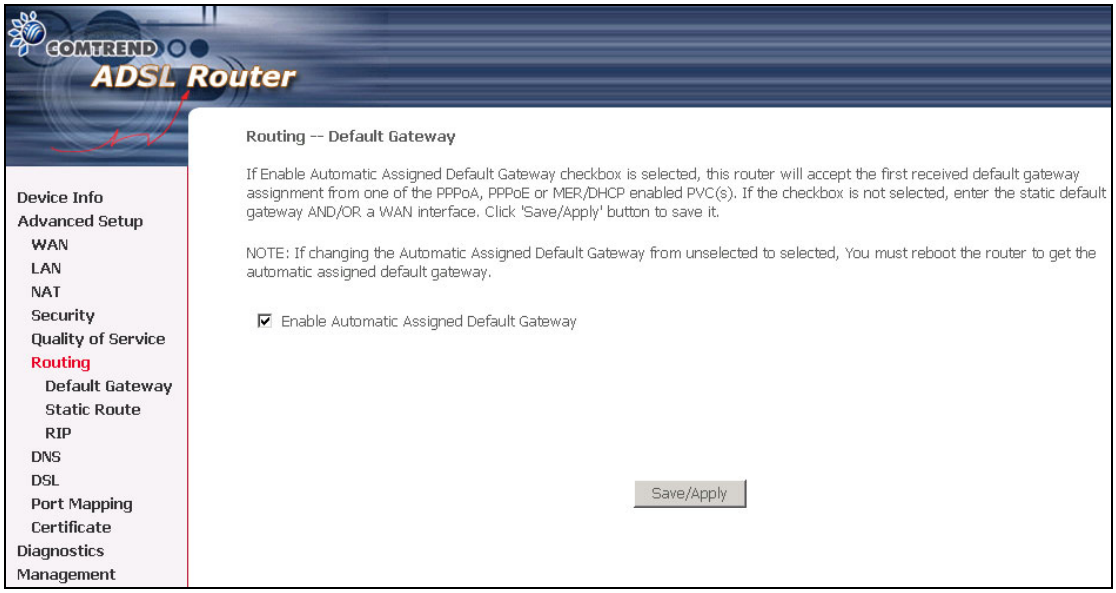
Chapter 6 Advanced Setup

This chapter explains: WAN, LAN, Routing, DSL and Port Mapping……

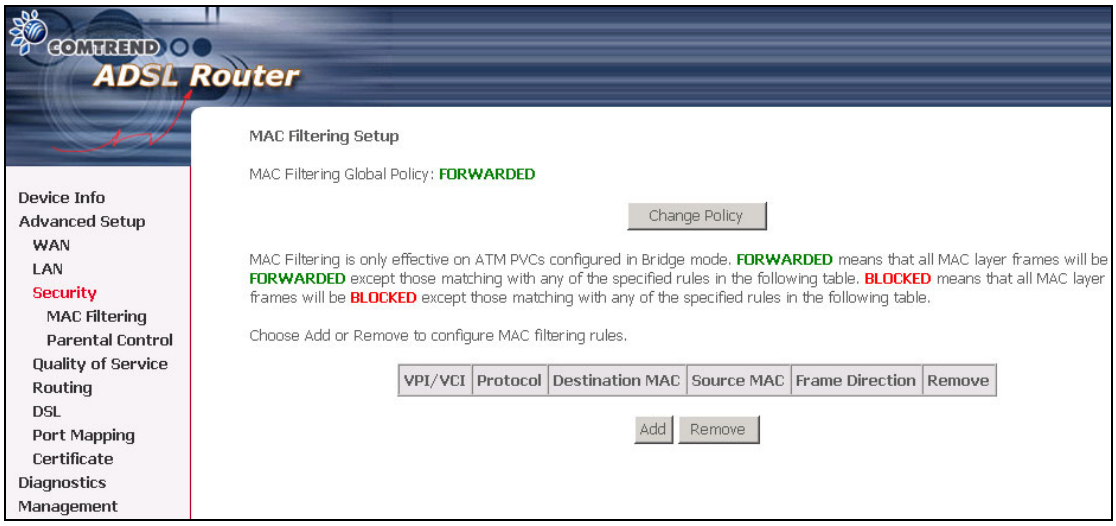
Note: Shown below for your reference are the available menu options for each different configuration.



This screenshot is for Mer and IPoA encapsulations.

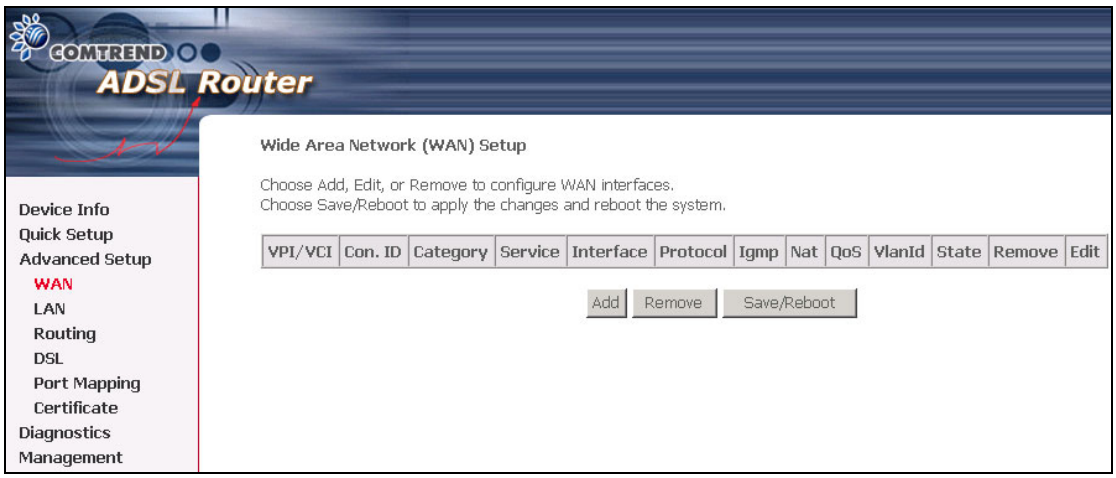

COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
Default Gateway
Static Route
RIP
DNS
DSL
Port Mapping
Certificate
Diagnostics
Management
Routing -- Default Gateway
If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.
NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.
Enable Automatic Assigned Default Gateway
Save/Apply

This screenshot is for PPPoE and PPPoA encapsulations.



This screenshot is for Bridge encapsulation.

6.1 WAN



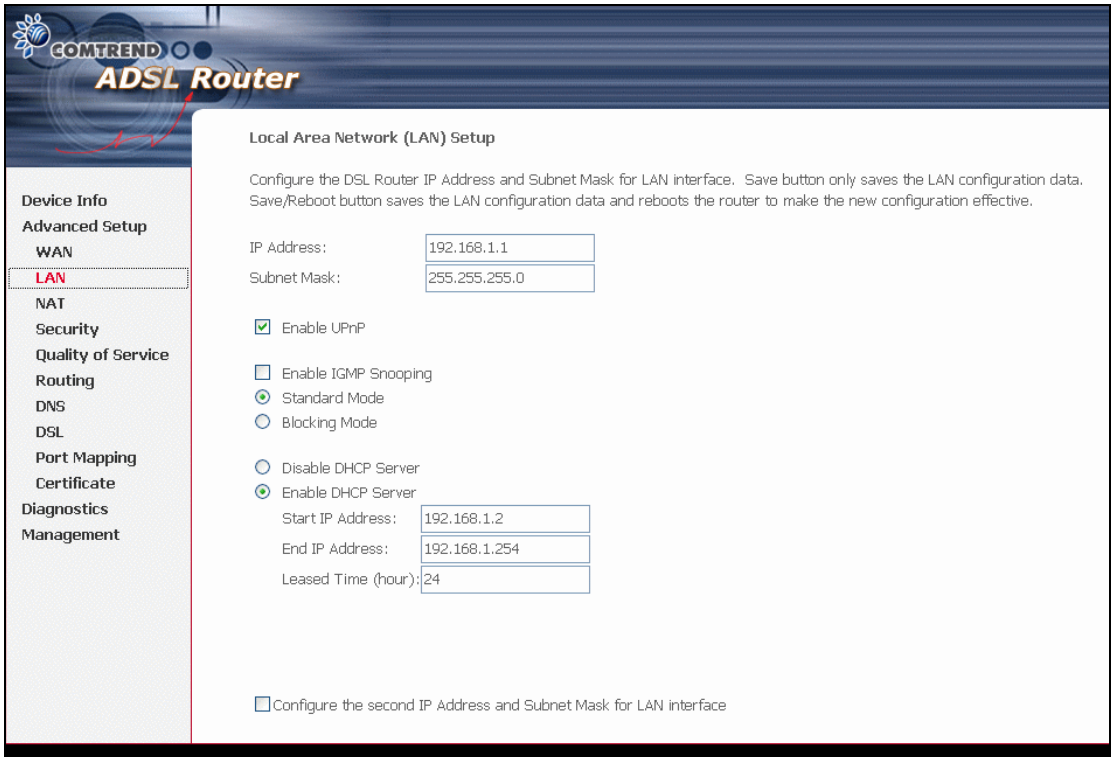
VlanID	• This function means one can add an 802.1Q VLAN tag on PPPoE/MER or Bridge mode. It means the packets are sent to WAN and a specific VlanID (802.1Q tag) will be added in the Ethernet header. The VlanID shows which 802.1Q tag will be added.

Please reference Section 4.1 for further information.

6.2 LAN

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address: Enter the IP address for the LAN port.
Subnet Mask: Enter the subnet mask for the LAN port.

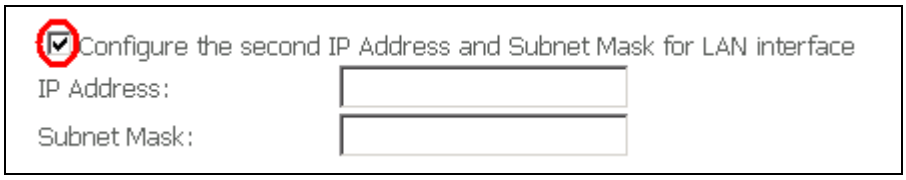


Enable IGMP Snooping: Enable /Disable the function that is IGMP Snooping.

Standard Mode: In standard mode, as in all prior releases, multicast traffic will flood to all bridge ports when there is no client subscribes to any multicast group – even when IGMP snooping is enabled.

Blocking Mode: In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there is no client subscription to any multicast group.

To configure a secondary IP address for the LAN port, click the box as shown below.



IP Address: Enter the secondary IP address for the LAN port.

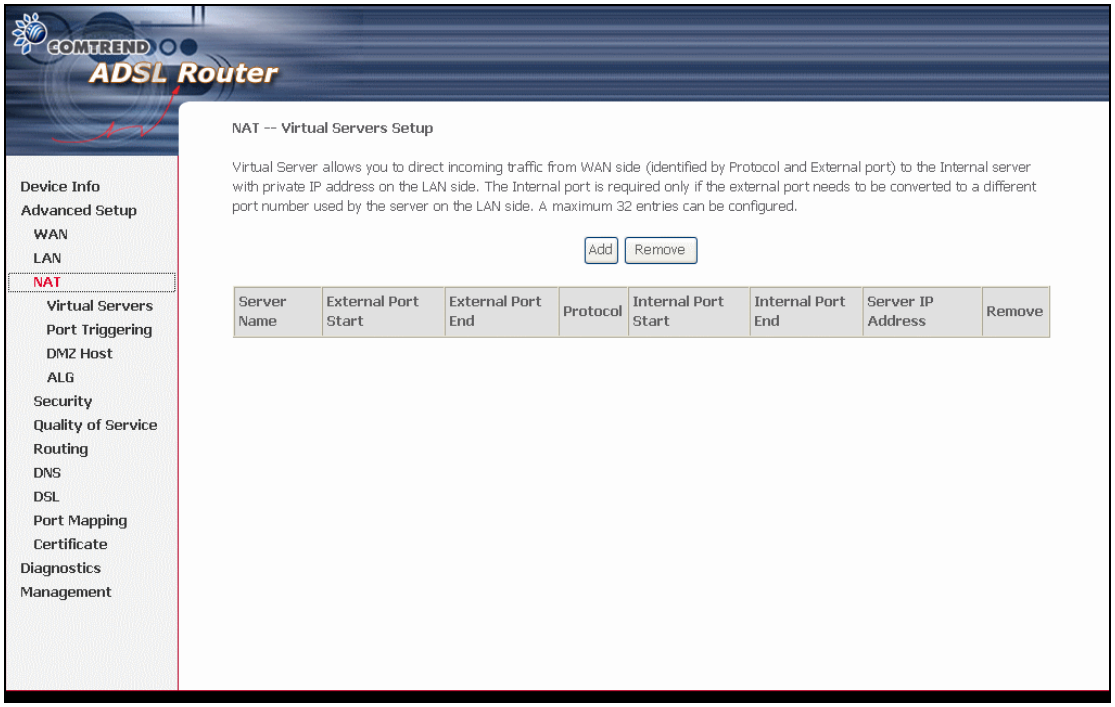
Subnet Mask: Enter the secondary subnet mask for the LAN port.

6.3 NAT

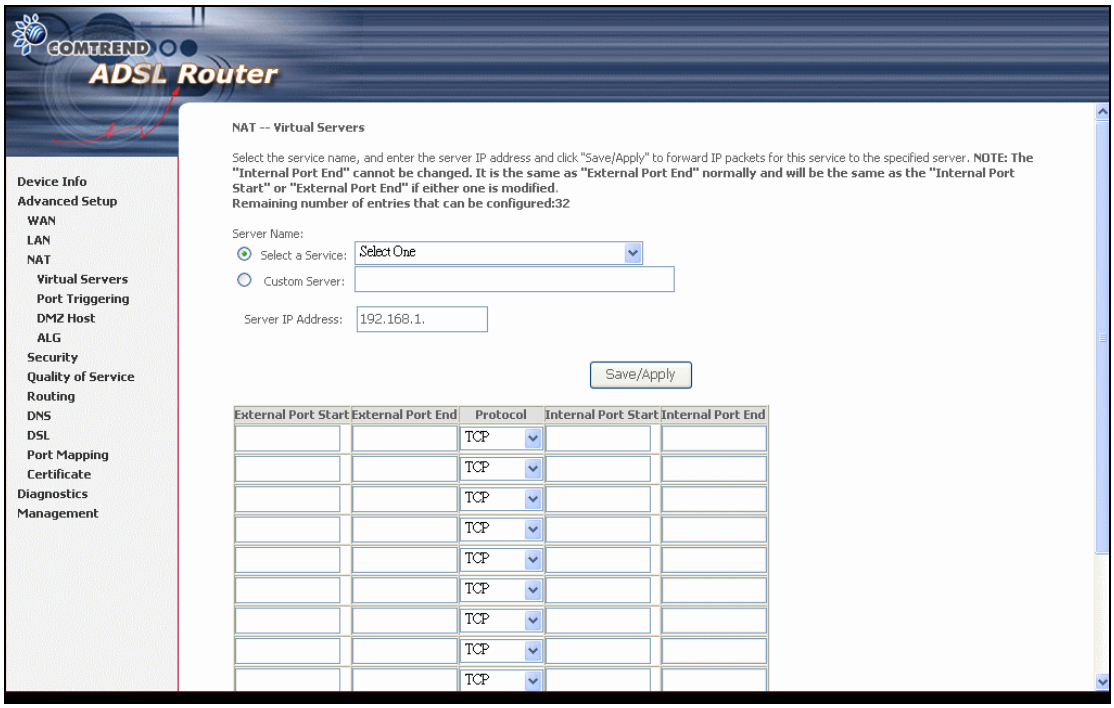
To display the NAT function, you need to enable the NAT feature in the WAN Setup.

6.3.1 Virtual Servers

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.



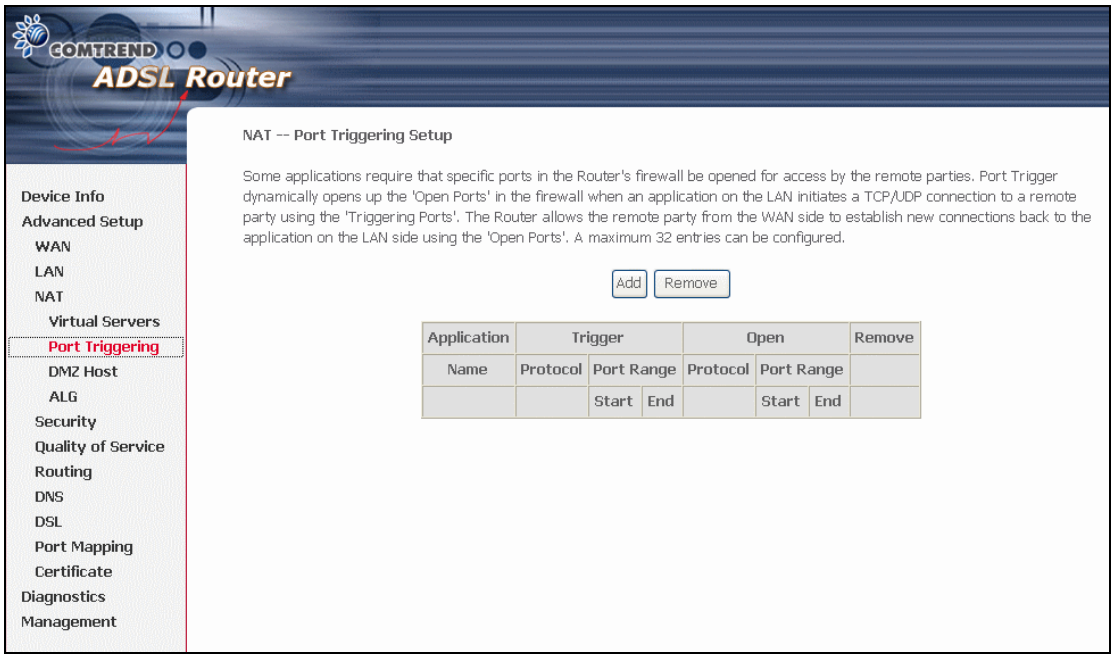
To add a Virtual Server, simply click the **Add** button. The following will be displayed.



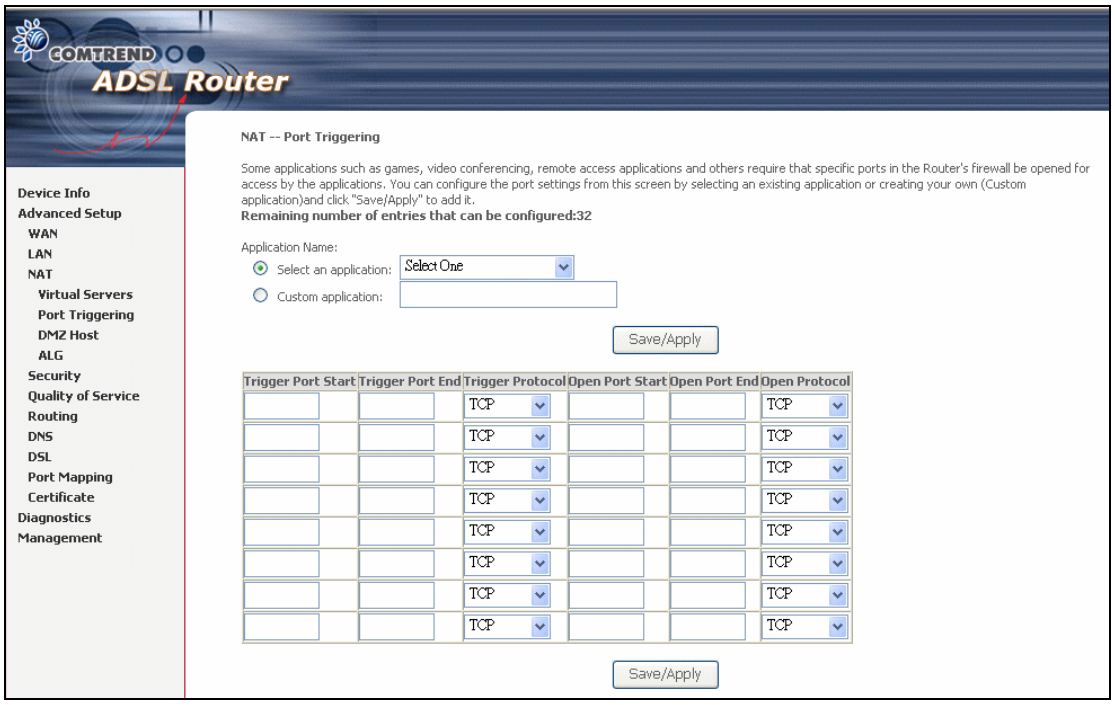
Select a Service Or Custom Server	User should select the service from the list. Or User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.

6.3.2 Port Triggering

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.



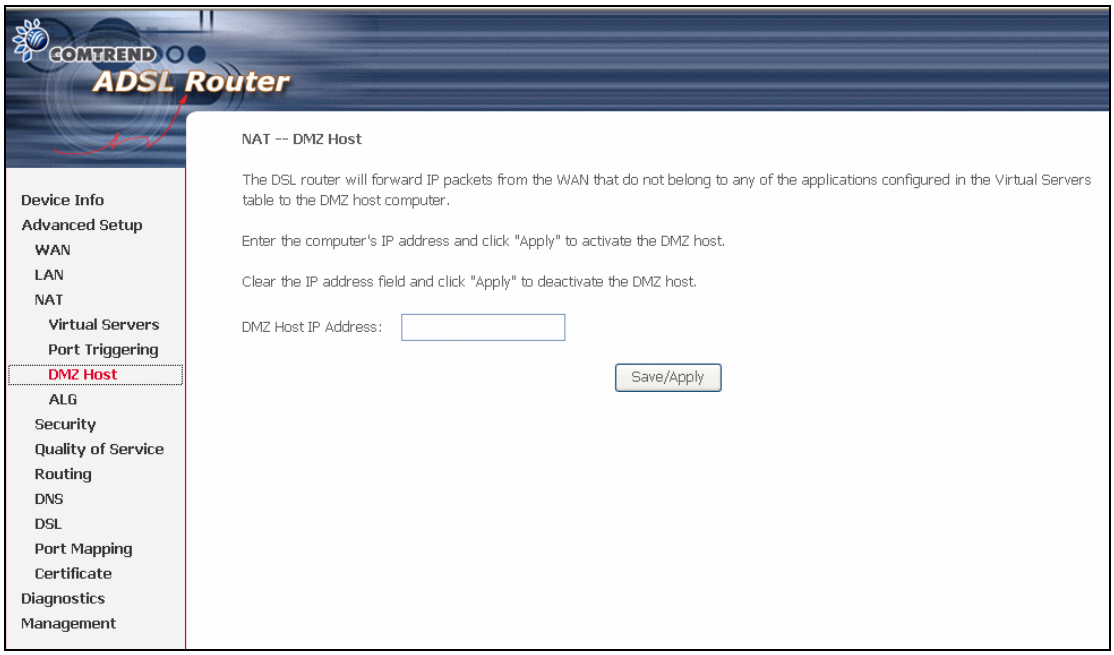
To add a Trigger Port, simply click the Add button. The following will be displayed.



Select an Application **Or** Custom Application	User should select the application from the list. **Or** User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Protocol	User can select from: TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Protocol	User can select from: TCP, TCP/UDP or UDP.

6.3.3 DMZ Host

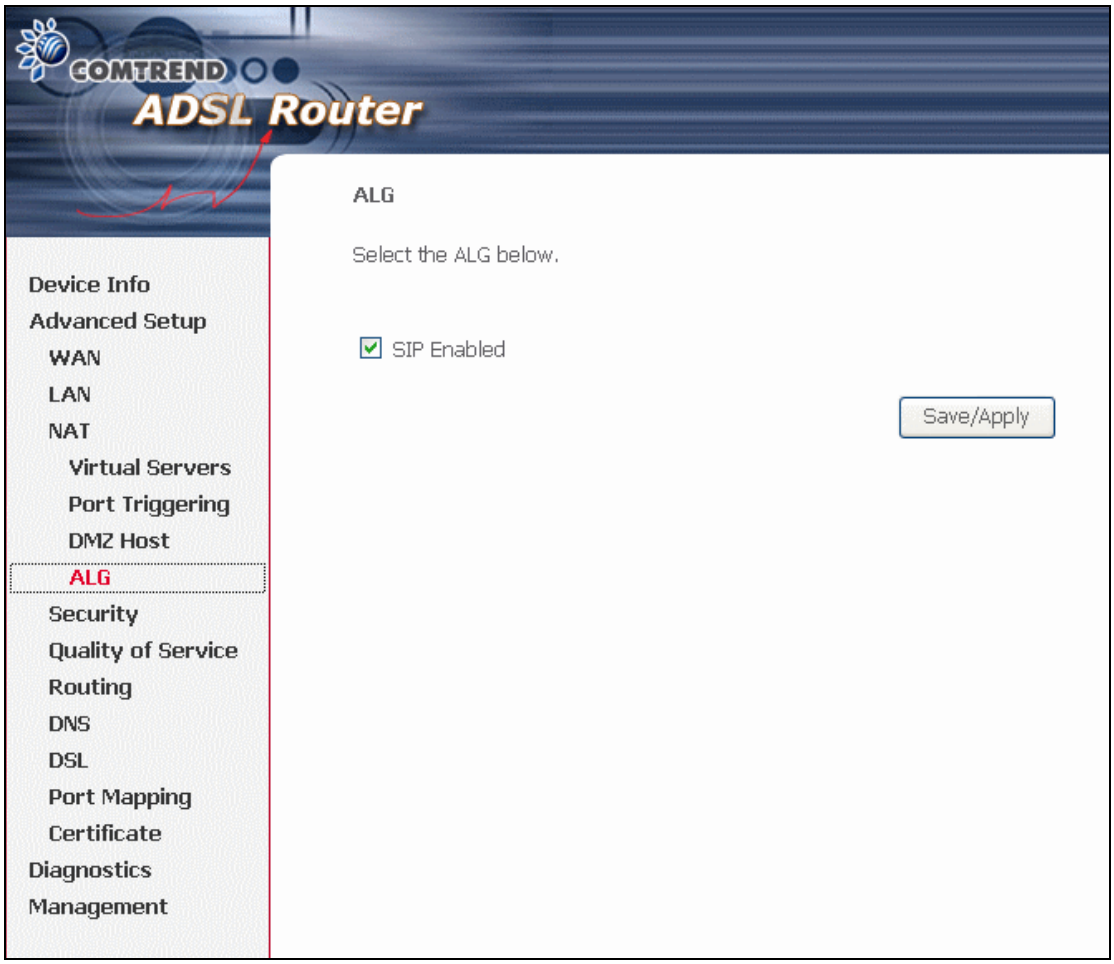
The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.



Enter the computer's IP address and click "Apply" to activate the DMZ host.
Clear the IP address field and click "Apply" to deactivate the DMZ host.

6.3.4 ALG

SIP ALG is Application layer gateway. If the user has an IP phone(SIP) or VoIP gateway(SIP) behind the ADSL router, the SIP ALG can help VoIP packet passthrough the router (NAT enabled).



Note: SIP (Session Initiation Protocol, RFC3261) is the protocol of choice for most VoIP (Voice over IP) phones to initiate communication. This ALG is only valid for SIP protocol running on UDP port 5060.

6.4 Security

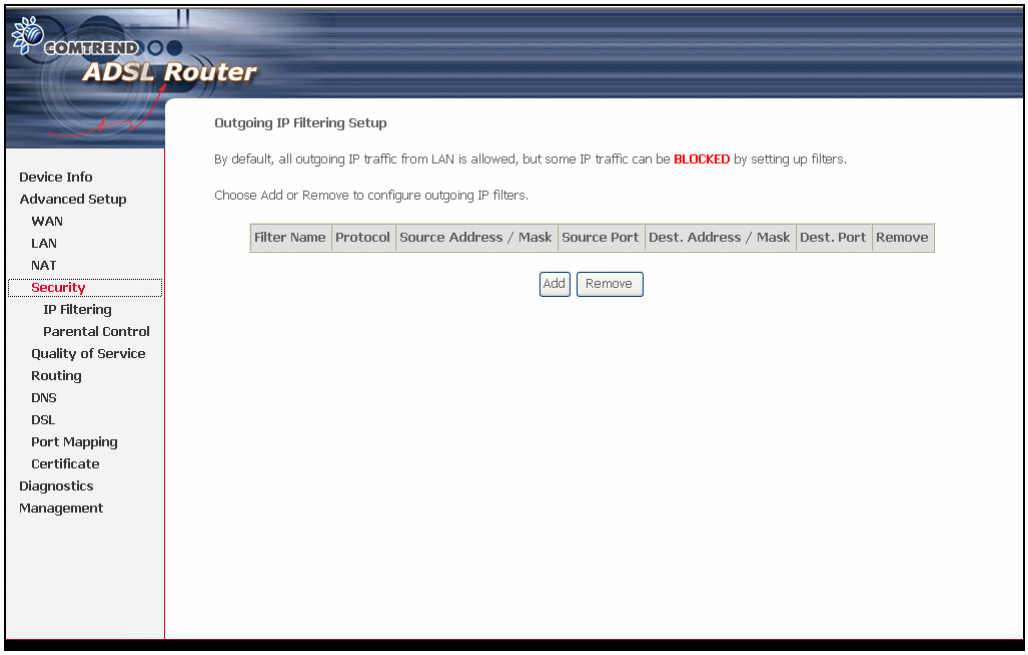
To display the Security function, you need to enable the firewall feature in the WAN Setup.

6.4.1 IP Filtering

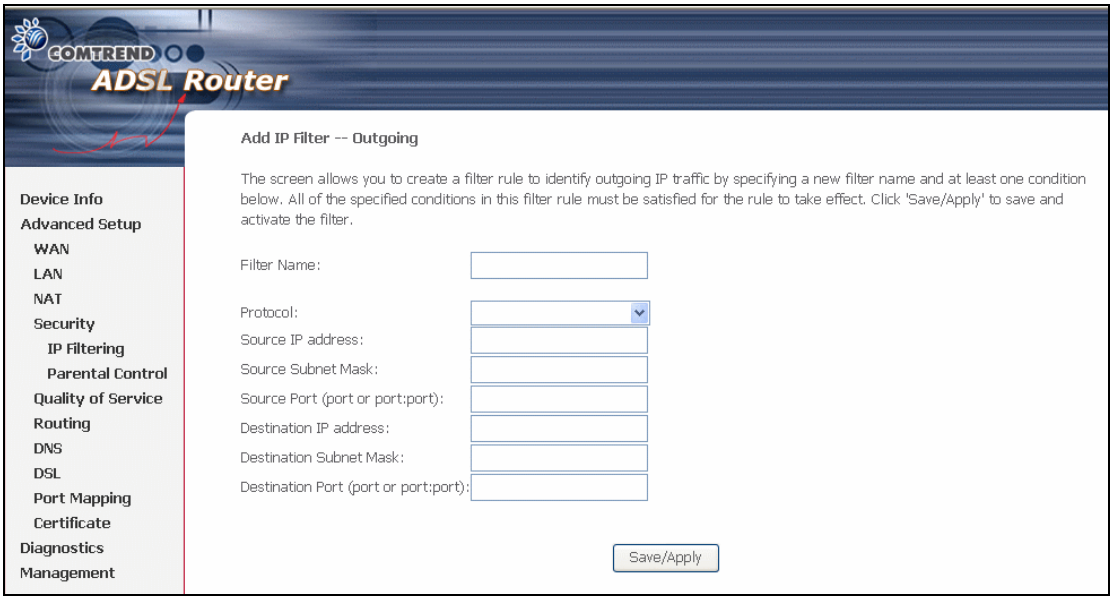
IP filtering allows you to create a filter rule to identify outgoing/incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Outgoing

Note: The default setting for Outgoing is Accepted.



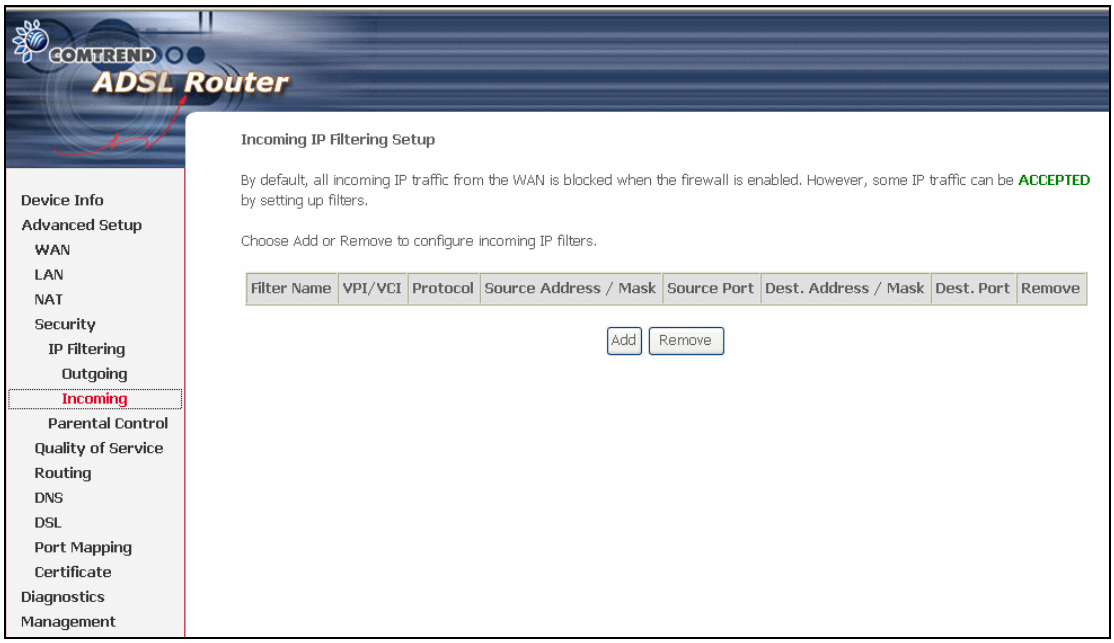
To add a filtering rule, simply click the Add button. The following screen will be displayed.



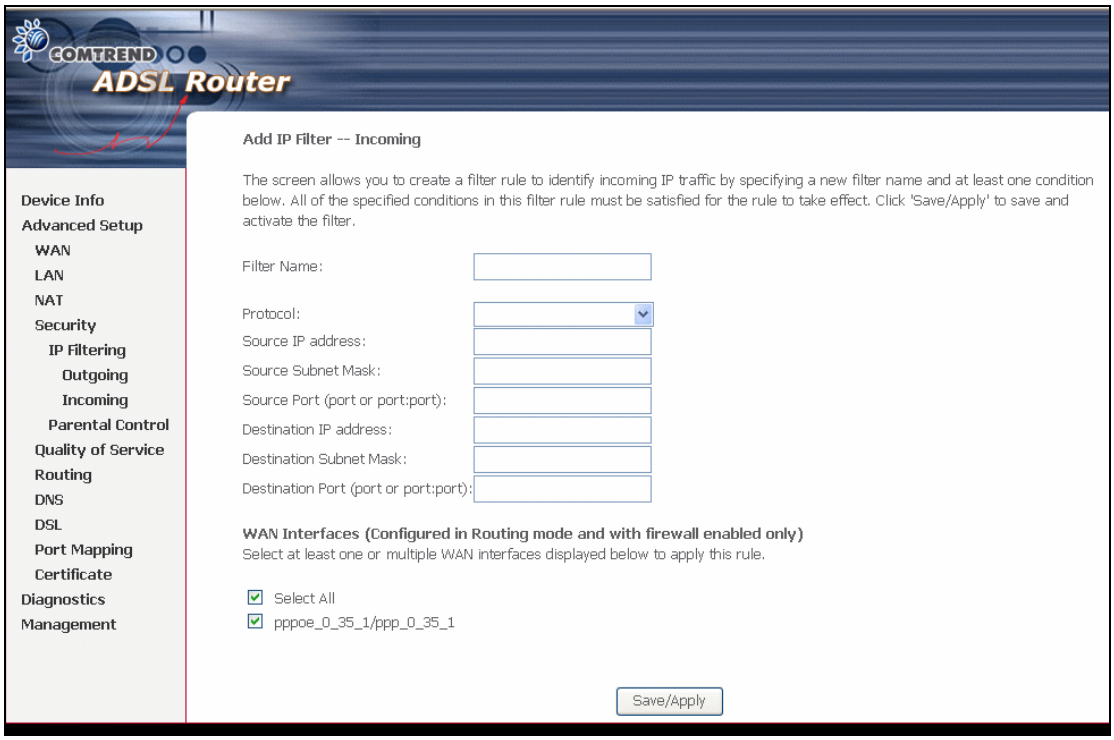
Filter Name	Type a name for the filter rule.
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.
Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.

Incoming

Note: The default setting for Incoming is Blocked.



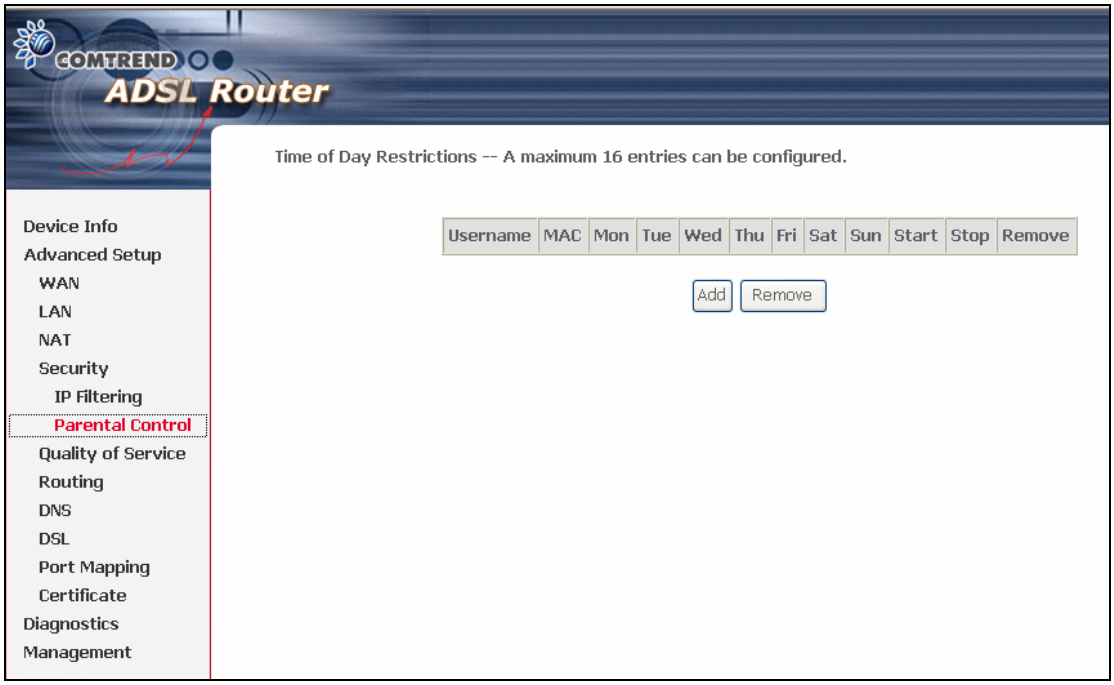
To add a filtering rule, simply click the Add button. The following screen will be displayed.


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
IP Filtering
Outgoing
Incoming
Parental Control
Quality of Service
Routing
DNS
DSL
Port Mapping
Certificate
Diagnostics
Management
Add IP Filter -- Incoming
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.
Filter Name:
Protocol:
Source IP address:
Source Subnet Mask:
Source Port (port or port:port):
Destination IP address:
Destination Subnet Mask:
Destination Port (port or port:port):
WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.
Select All
pppoe_0_35_1/ppp_0_35_1
Save/Apply

To configure the parameters, please reference **Outgoing** table above.

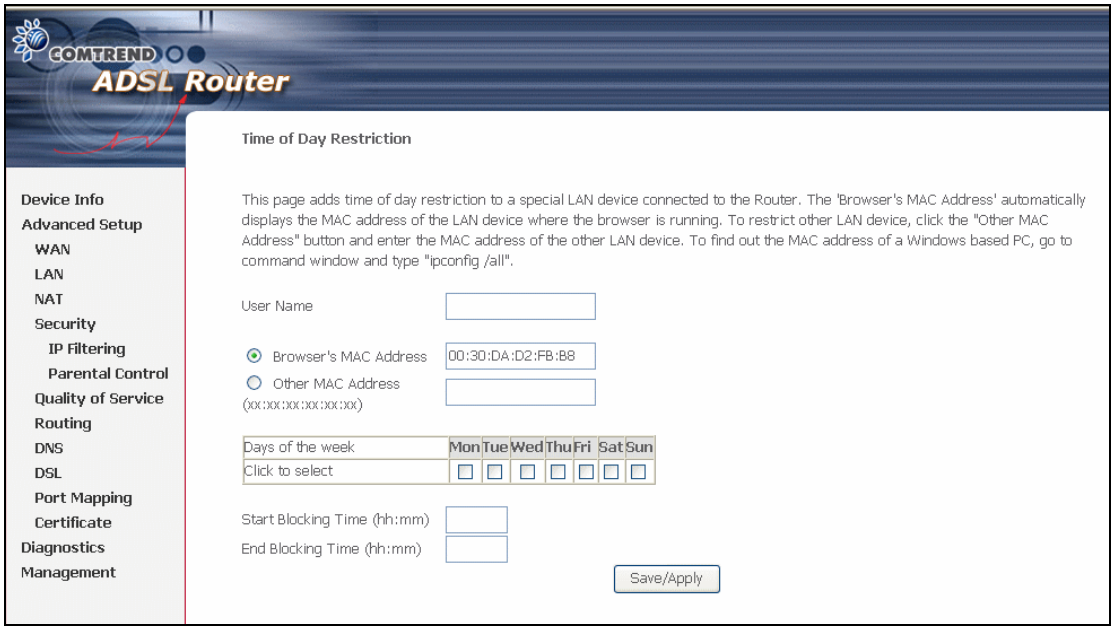
6.4.2 Parental Control

Parental control: allows parents, schools, and libraries to set access times for Internet use.



To add a parental control, simply click the Add button.

The following screen will be displayed.


COMTREND
ADSL Router
Time of Day Restriction
This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".
Device Info
Advanced Setup
WAN
LAN
NAT
Security
IP Filtering
Parental Control
Quality of Service
Routing
DNS
DSL
Port Mapping
Certificate
Diagnostics
Management
User Name
Browser's MAC Address
00:30:DA:D2:FB:B8
Other MAC Address
(xx:xx:xx:xx:xx:xx)
Days of the week
Mon Tue Wed Thu Fri Sat Sun
Click to select
Start Blocking Time (hh:mm)
End Blocking Time (hh:mm)
Save/Apply

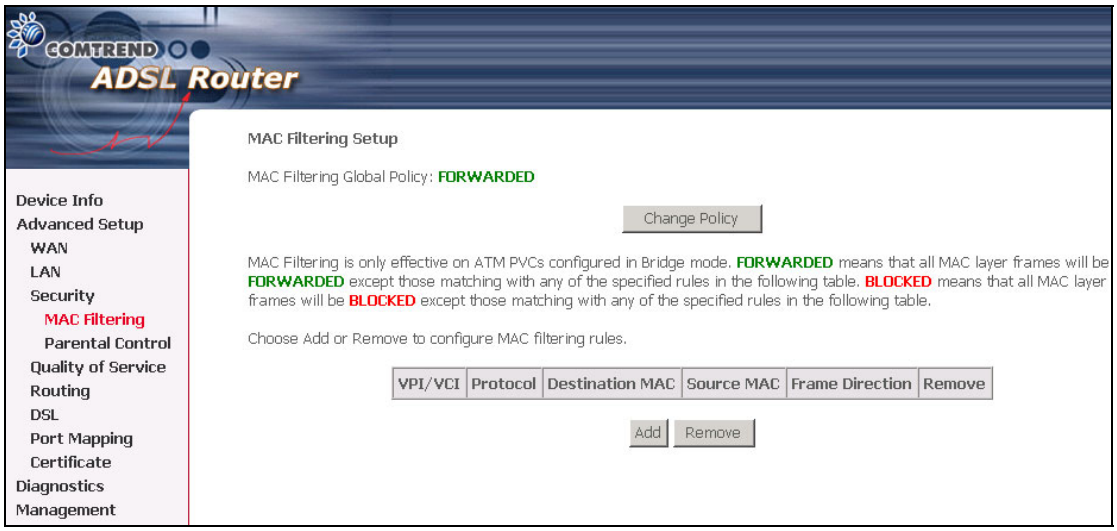
Username:	Input Internet access user name
MAC:	Set the MAC address to access the Internet
Mon, Tue, Wed, Thu, Fri, Sat, Sun:	Set which days that will have block restrictions to Internet access
Start, End Blocking Time:	Set Internet block start and stop time

6.4.3 MAC Filtering

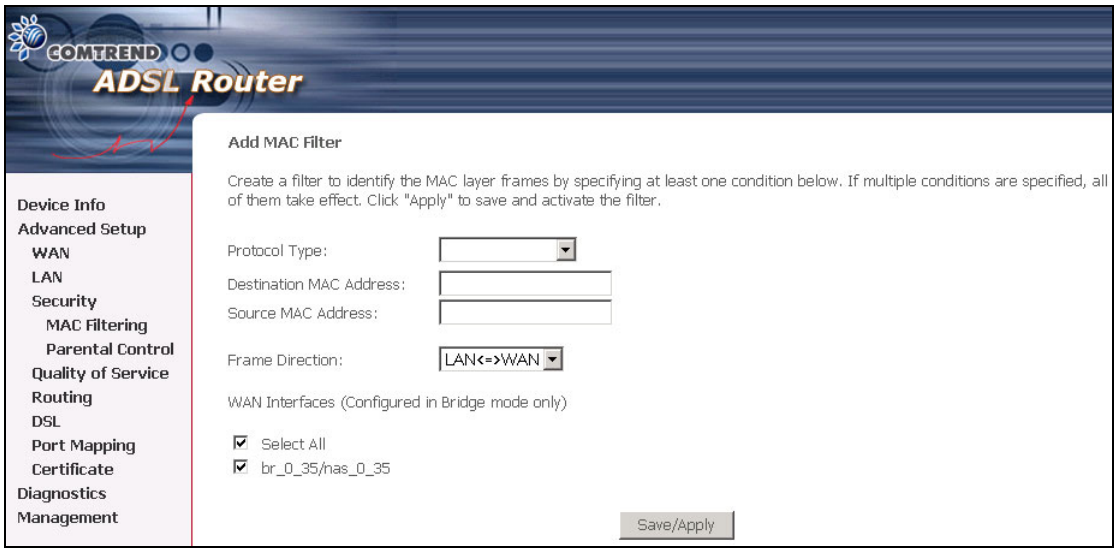
Mac Filtering is only available when Bridging PVC is configured.

Each network device has a unique MAC address. You can block or forward the packets based on the MAC addresses. The MAC Filtering Setup screen allows setting up the MAC filtering policy and the MAC filtering rules. MAC Filtering is only effective on ATM PVCs configured in Bridge mode.

The policy **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table. The default is FORWARD; you change by clicking the **Change Policy** button.



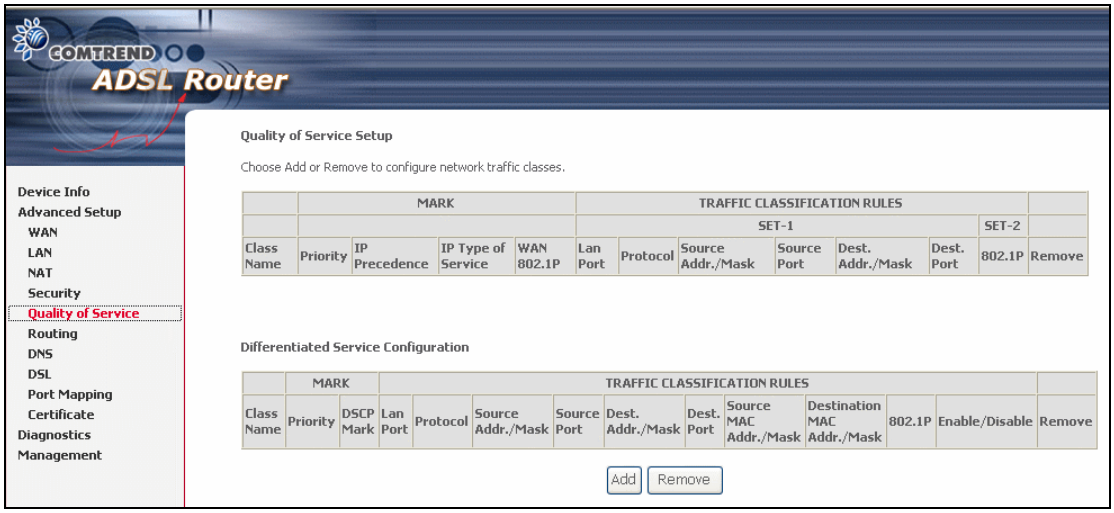
Choose **Add** or **Remove** to configure MAC filtering rules. The following screen pops up when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click **Apply** to save and activate the filter.



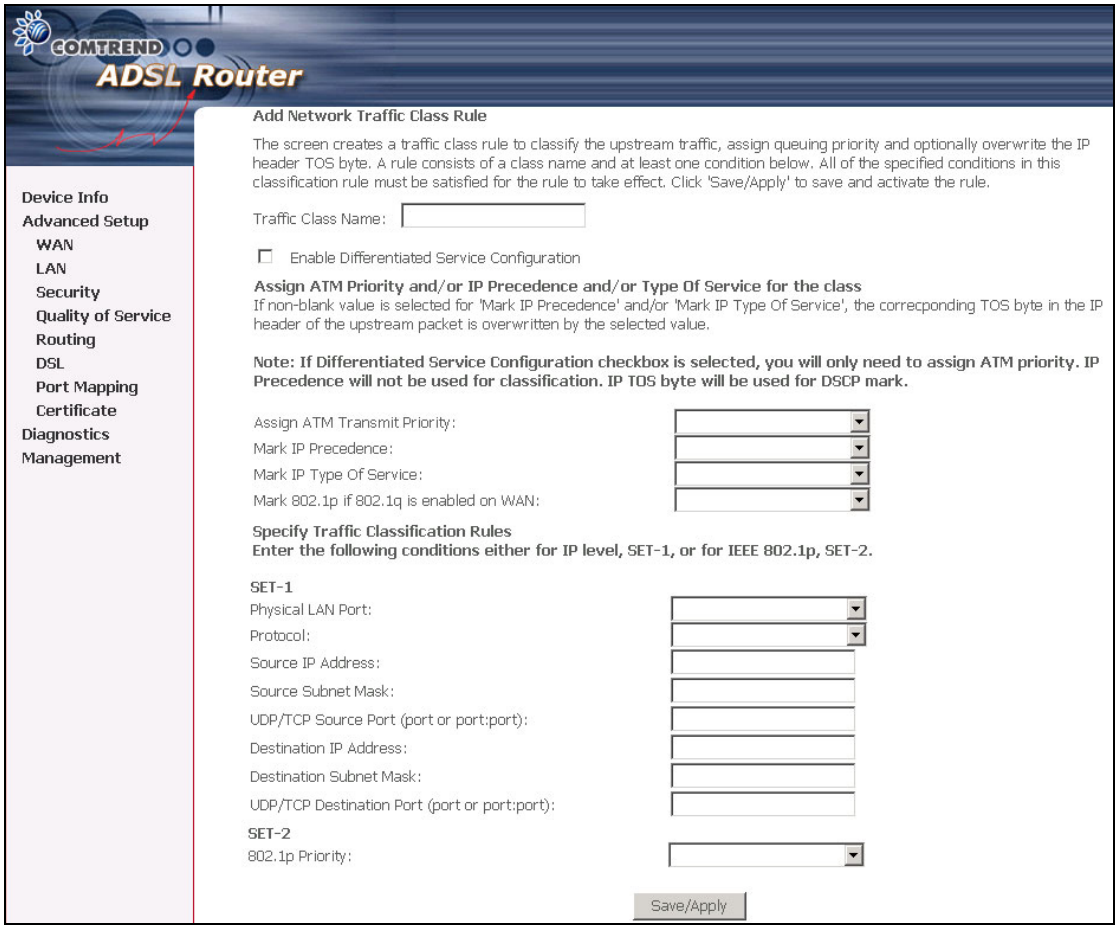
Option	Description
Protocol type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Define the destination MAC address
Source MAC Address	Define the source MAC address
Frame Direction:	Select a direction of the frame
WAN Interface	Selects the interface that the MAC filter rule(s) will be applied. Only the WAN interface that is configured for bridged can be selected. ☑ Select All ☑ br_0_35/nas_0_35

6.5 Quality of Service

To display the QoS function, you need to enable the QoS feature in the WAN Setup.

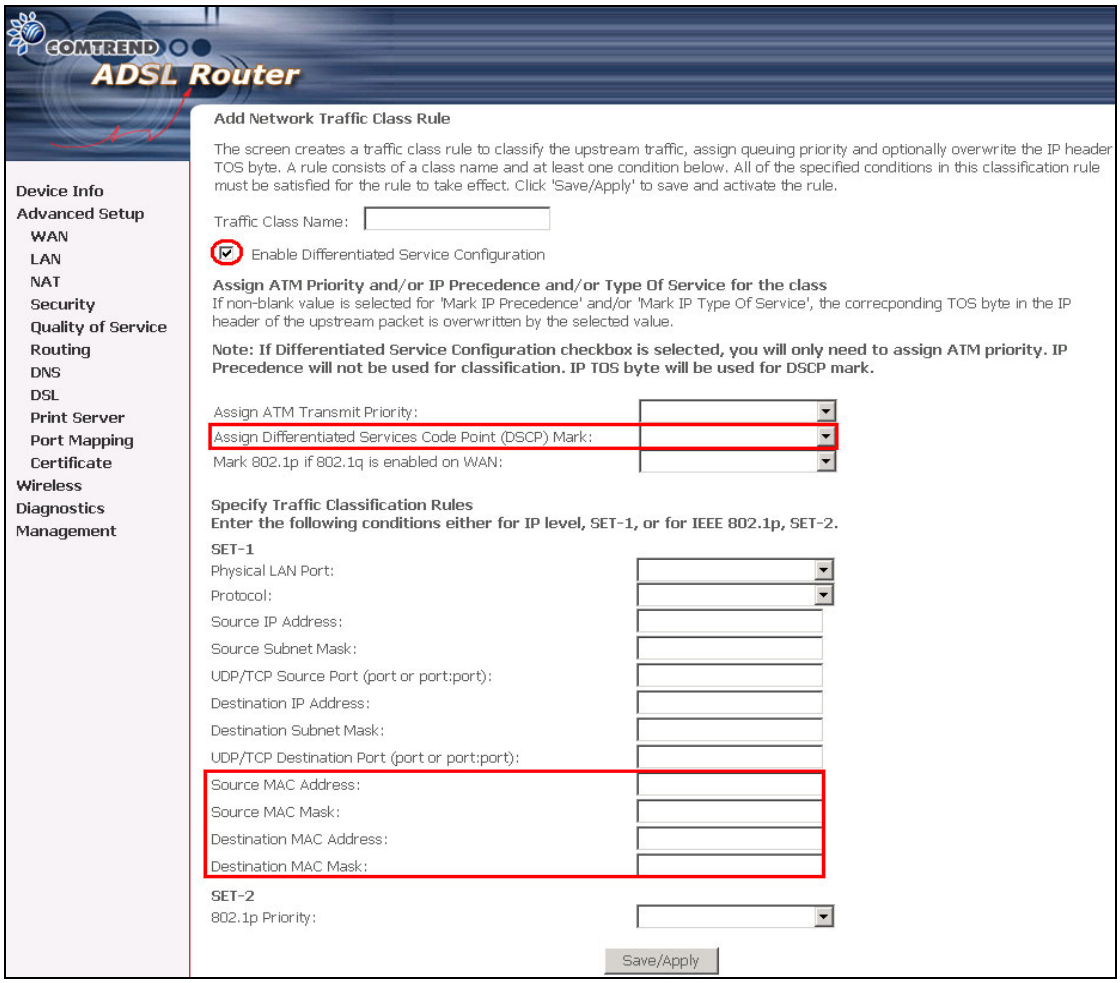


Choose **Add** to configure network traffic classes. The following screen will be displayed:


COMTREND
ADSL Router
Add Network Traffic Class Rule
The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.
Device Info
Advanced Setup
WAN
LAN
Security
Quality of Service
Routing
DSL
Port Mapping
Certificate
Diagnostics
Management
Traffic Class Name:
Enable Differentiated Service Configuration
Assign ATM Priority and/or IP Precedence and/or Type Of Service for the class
If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the correcponding TOS byte in the IP header of the upstream packet is overwritten by the selected value.
Note: If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.
Assign ATM Transmit Priority:
Mark IP Precedence:
Mark IP Type Of Service:
Mark 802.1p if 802.1q is enabled on WAN:
Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.
SET-1
Physical LAN Port:
Protocol:
Source IP Address:
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
UDP/TCP Destination Port (port or port:port):
SET-2
802.1p Priority:
Save/Apply

Traffic Class Name	Enter name for traffic class.
Assign ATM Transmit Priority	Select Low, Medium or High.
Mark IP Precedence	Select between 0-7. The lower the digit shows the higher the priority.
Mark IP Type Of Service	Select either: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay
Mark 802.1p if 802.1q is enabled on WAN	Select between 0-7. The higher the digit shows the higher the priority.
SET-1	
Physical LAN Port	Select between ENET(1-4) and USB
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the subnet mask for the source IP address.
Source Port (port or port:port)	Enter source port number or port range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number or port range.
SET-2	
802.1p Priority	Select between 0-7. The lower the digit shows the higher the priority

If the **Enable Differentiated Service Configuration** box is ticked (i.e. selected) the following screen will be displayed:


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Wireless
Diagnostics
Management
Add Network Traffic Class Rule
The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.
Traffic Class Name:
Enable Differentiated Service Configuration
Assign ATM Priority and/or IP Precedence and/or Type Of Service for the class
If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the correcponding TOS byte in the IP header of the upstream packet is overwritten by the selected value.
Note: If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.
Assign ATM Transmit Priority:
Assign Differentiated Services Code Point (DSCP) Mark:
Mark 802.1p if 802.1q is enabled on WAN:
Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.
SET-1
Physical LAN Port:
Protocol:
Source IP Address:
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
UDP/TCP Destination Port (port or port:port):
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:
SET-2
802.1p Priority:
Save/Apply

The additional Items are explained here.

Assign Differentiated Services Code Point (DSCP) Mark	The selected Code Point gives the corresponding priority to the packets that satisfies the rules set below.
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in Destination MAC Address.

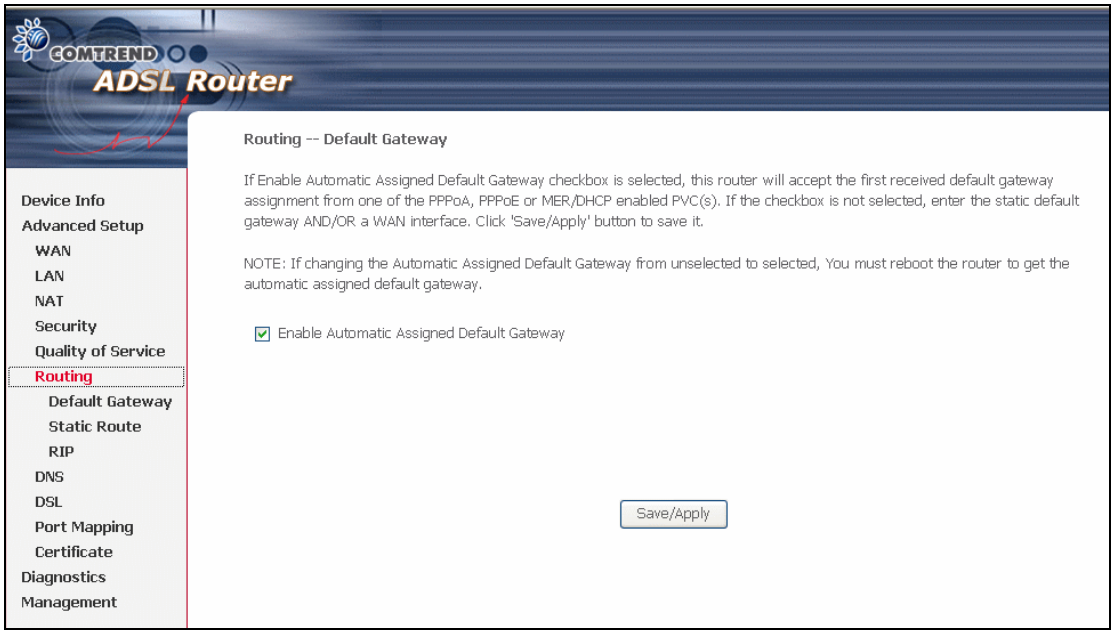
6.6 Routing

The Routing dialog box allows you to configure Default gateway, Static Route and RIP.

6.6.1 Default Gateway

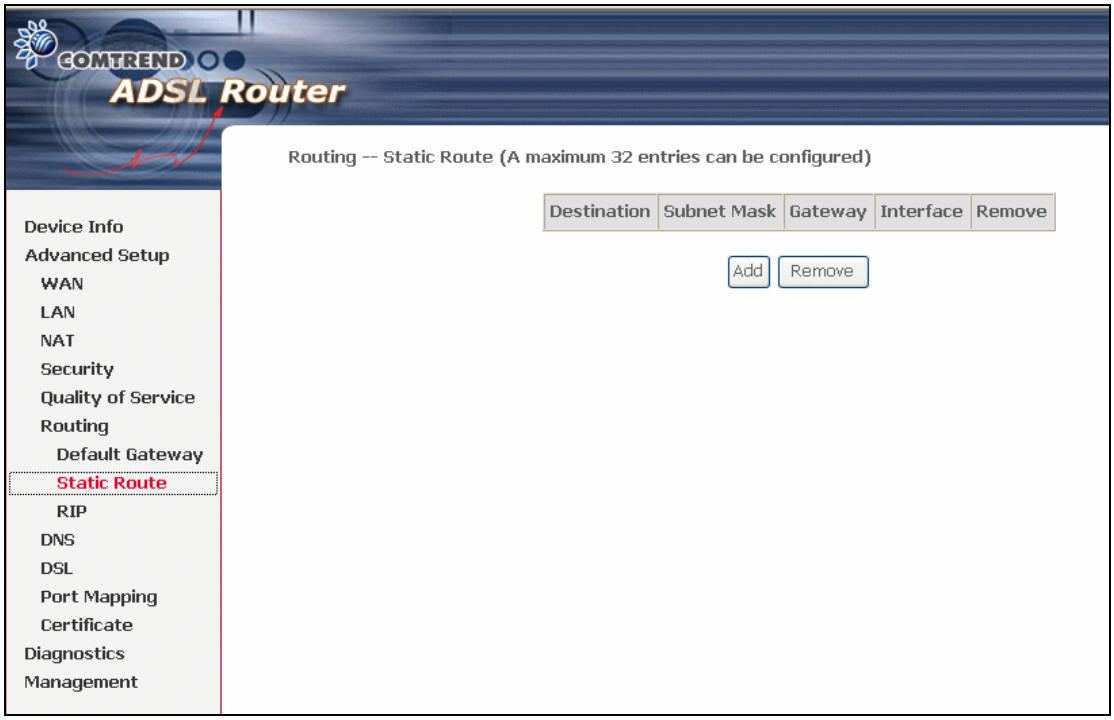
If '**Enable Automatic Assigned Default Gateway'** checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
Default Gateway
Static Route
RIP
DNS
DSL
Port Mapping
Certificate
Diagnostics
Management
Routing -- Default Gateway
If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.
NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.
Enable Automatic Assigned Default Gateway
Save/Apply

6.6.2 Static Route

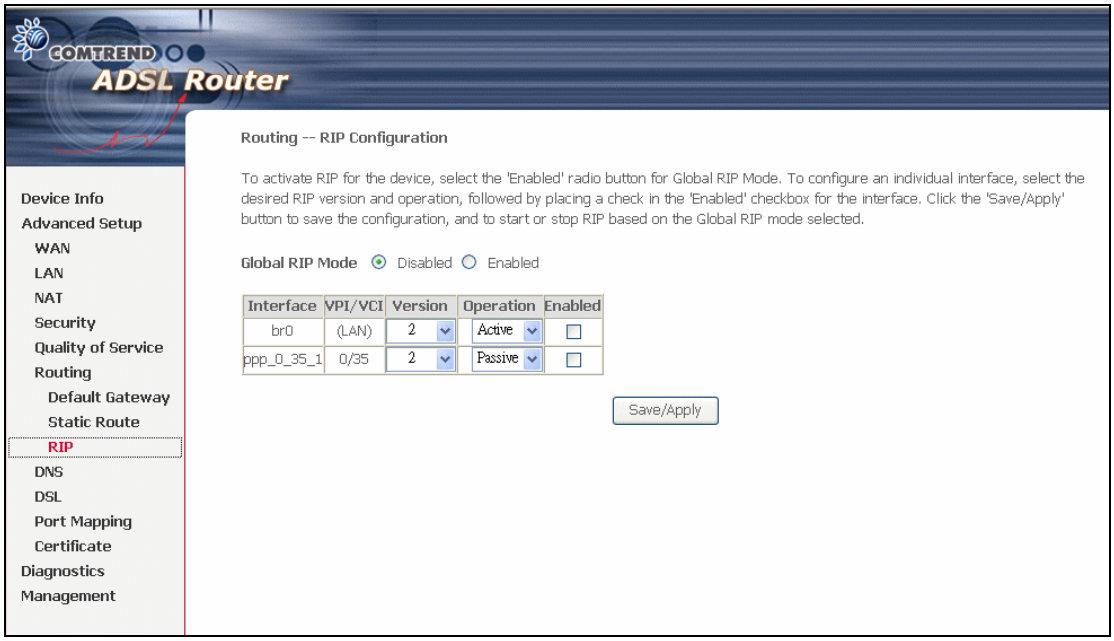
Choose **Static Route** to display the Static Route screen. The Static Route screen lists the configured static routes, and allows configuring static routes. Choose **Add** or **Remove** to configure the static routes.



To add static route, click the **Add** button to display the following screen. Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click **Save/Apply** to add the entry to the routing table.

6.6.3 RIP

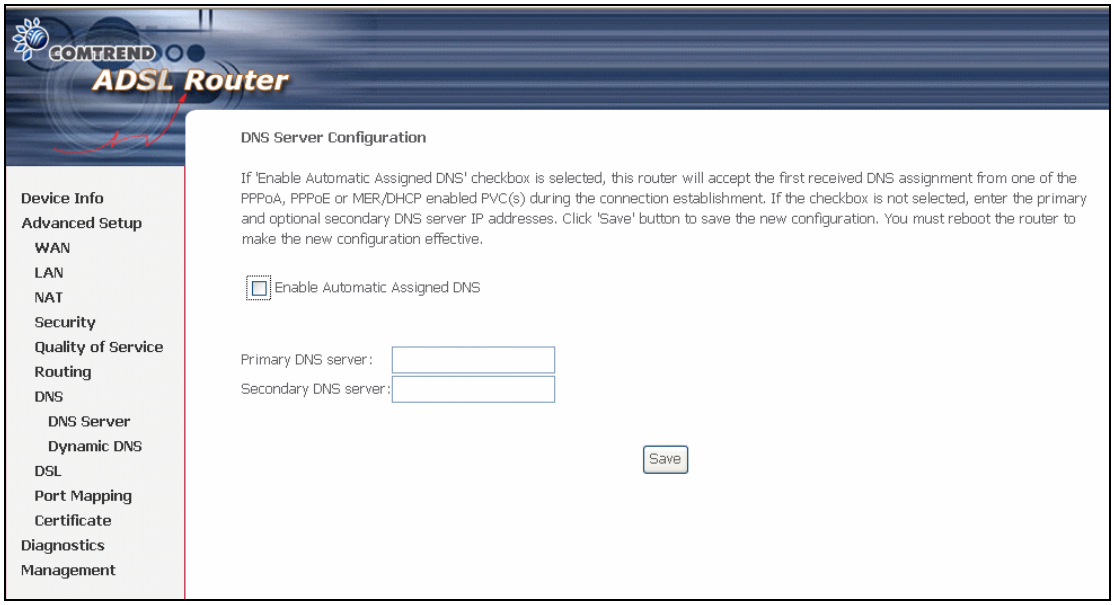
To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
Default Gateway
Static Route
RIP
DNS
DSL
Port Mapping
Certificate
Diagnostics
Management
Routing -- RIP Configuration
To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.
Global RIP Mode Disabled Enabled
Interface VPI/VCI Version Operation Enabled
br0 (LAN) 2 Active
ppp_0_35_1 0/35 2 Passive
Save/Apply

6.7 DNS

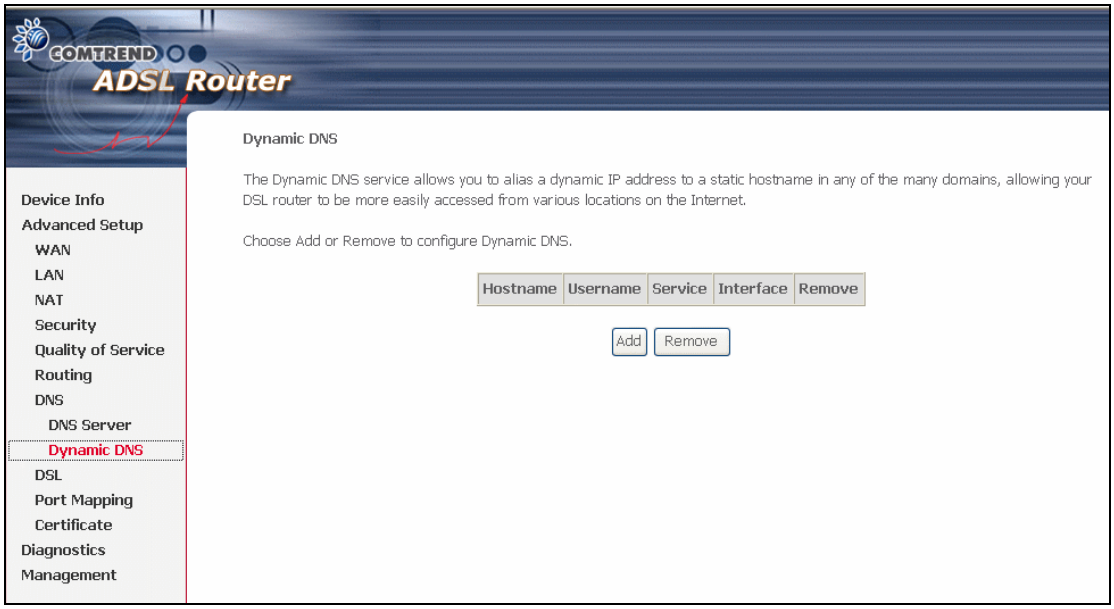
6.7.1 DNS Server

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DSL
Port Mapping
Certificate
Diagnostics
Management
DNS Server Configuration
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.
Enable Automatic Assigned DNS
Primary DNS server:
Secondary DNS server:
Save

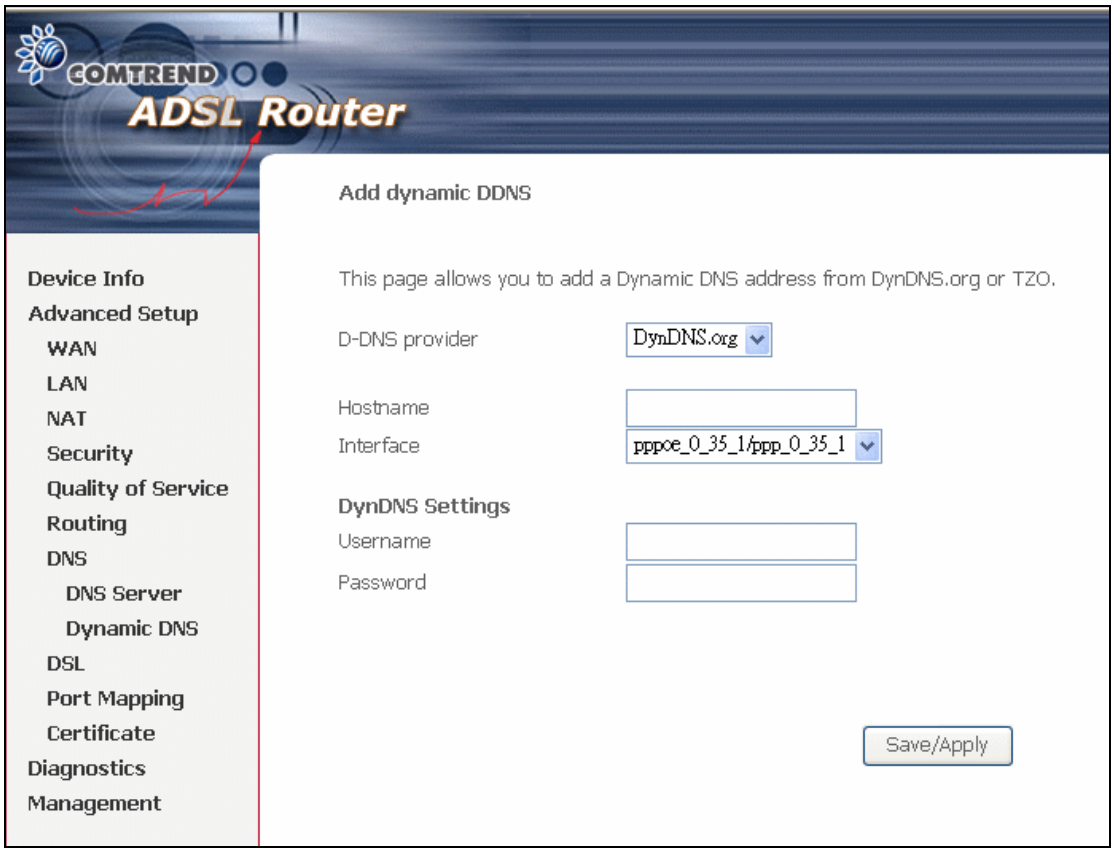
6.7.2 Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.



To add a dynamic DNS service, simply click the Add button.

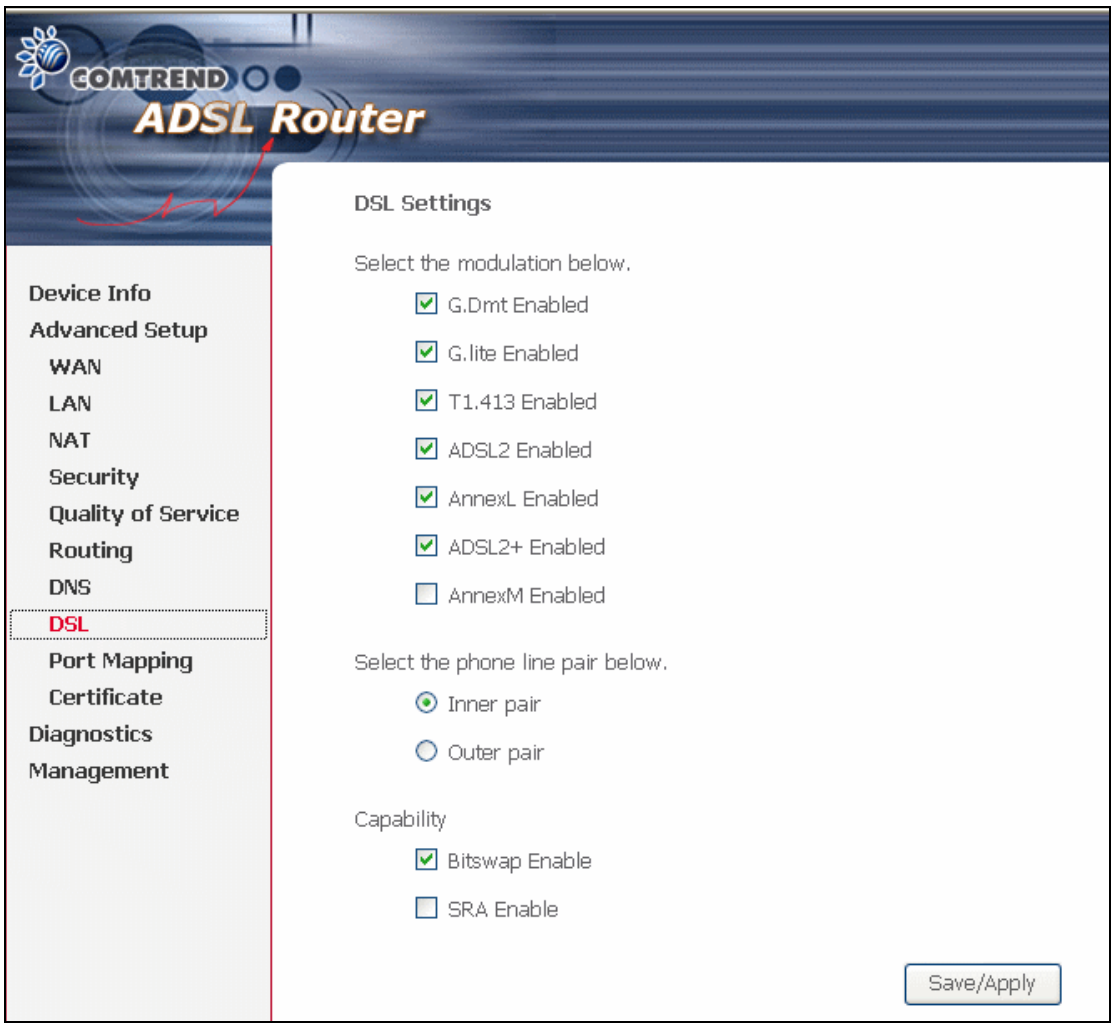
The following screen will be displayed:



D-DNS provider	Select a dynamic DNS provider from the list.
Hostname	Enter the name for the dynamic DNS server.
Interface	Select the interface from the list.
Username	Enter the username for the dynamic DNS server.
Password	Enter the password for the dynamic DNS server.

6.8 DSL

To access the DSL settings, first click On **Advanced Setup** and then click on **DSL**. The DSL Settings dialog box allows you to select an appropriate modulation mode.



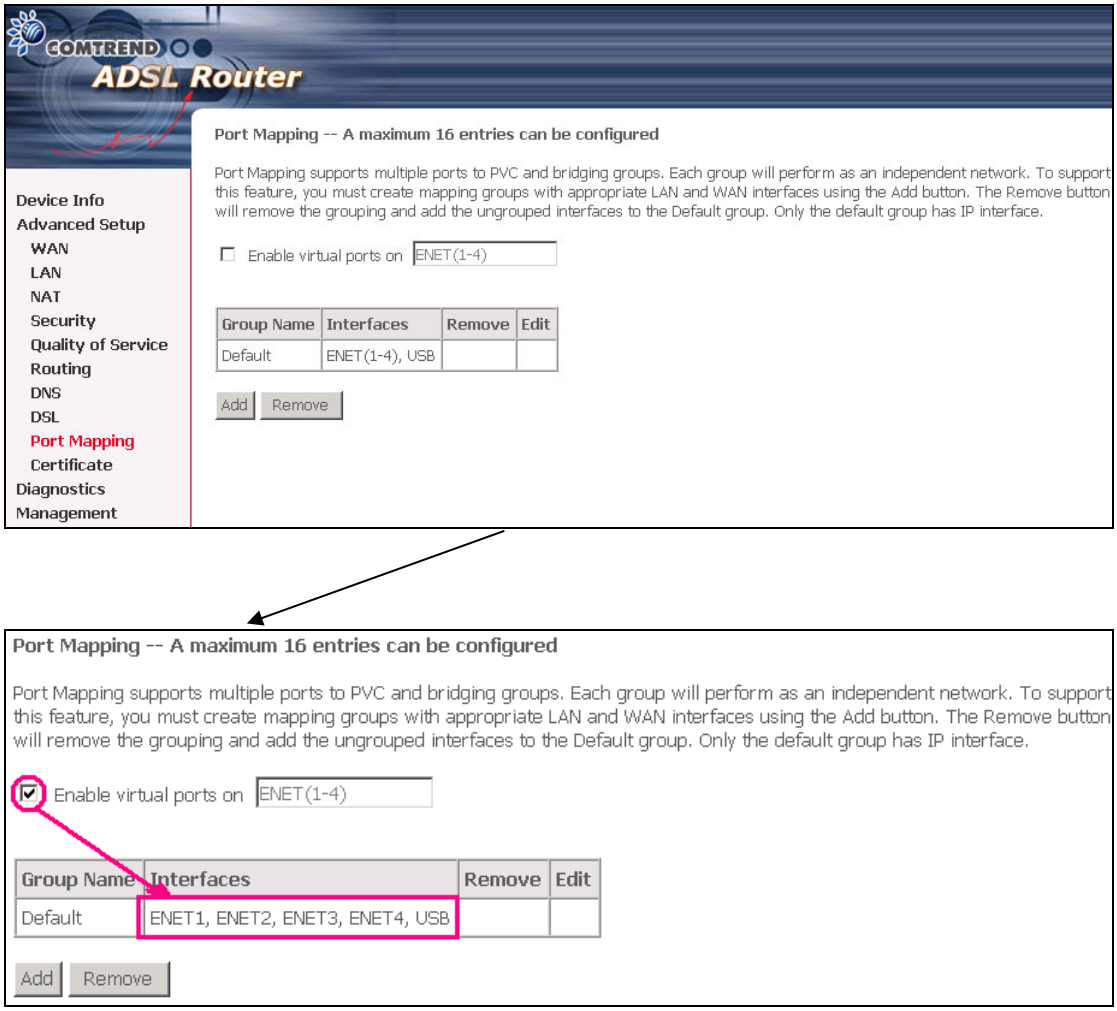
Option	Description
G.dmt Enabled	Sets G.Dmt if you want the system to use G.Dmt mode.
G.Lite Enabled	Sets G.Lite if you want the system to use G.Lite mode.
T1.413 Enabled	Sets the T1.413 if you want the system to use only T1.413 mode.
ADSL2 Enabled	The device can support the functions of the ADSL2.
AnnexL Enabled	The device can support/enhance the long loop test.
ADSL2+ Enabled	The device can support the functions of the ADSL2+.
AnnexM ENABLED	Covers a higher "upstream" data rate version, by making use of some of the downstream channels.

Inner Pair	Reserved only
Outer Pair	Reserved only
Bitswap Enable	Allows bitswapping function
SRA Enable	Allows seamless rate adaptation

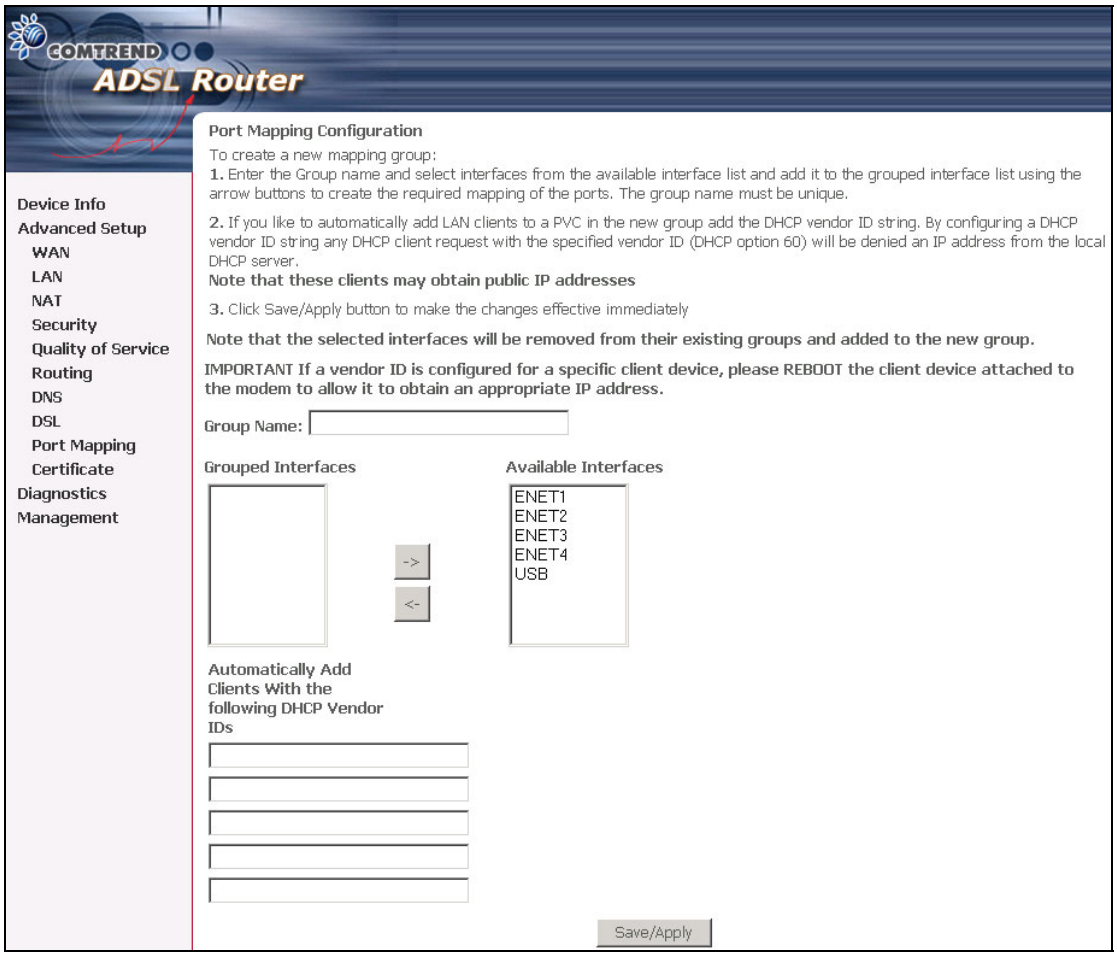
6.9 Port Mapping

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group.

As shown below, when you tick the Enable virtual ports on, all of the LAN interfaces will be grouped together as a default.


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Port Mapping
Certificate
Diagnostics
Management
Port Mapping -- A maximum 16 entries can be configured
Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.
Enable virtual ports on
ENET(1-4)
Group Name
Interfaces
Remove
Edit
Default
ENET(1-4), USB
Add
Remove
Port Mapping -- A maximum 16 entries can be configured
Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.
Enable virtual ports on
ENET(1-4)
Group Name
Interfaces
Remove
Edit
Default
ENET1, ENET2, ENET3, ENET4, USB
Add
Remove

To add a port mapping group, simply click the Add button.


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Port Mapping
Certificate
Diagnostics
Management
Port Mapping Configuration
To create a new mapping group:
1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
Note that these clients may obtain public IP addresses
3. Click Save/Apply button to make the changes effective immediately
Note that the selected interfaces will be removed from their existing groups and added to the new group.
IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.
Group Name:
Grouped Interfaces
Available Interfaces
ENET1
ENET2
ENET3
ENET4
USB
->
<-
Automatically Add Clients With the following DHCP Vendor IDs
Save/Apply

To create a group from the list, first enter the group name and then select from the available interfaces on the list.

Automatically Add Clients With the Following DHCP Vendor IDs:
Add support to automatically map LAN interfaces including USB to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when PortMapping is enabled.

There are 4 PVCs (0/33, 0/36, 0/37, 0/38). 0/33 is for PPPoE and the others are for IP setup-box (video). The LAN interfaces are ETH1, ETH2, ETH3, ETH4 and USB.

Port mapping configuration is:
1. Default: ETH1, ETH2, ETH3, ETH4 and USB.
2. Video: nas_0_36, nas_0_37 and nas_0_38. The DHCP vendor ID is "Video".

The CPE DHCP server is running on "Default". And ISP's DHCP server is running on PVC 0/36. It is for setup-box use only.

In the LAN side, PC can get IP address from CPE DHCP server and access Internet via PPPoE (0/33).

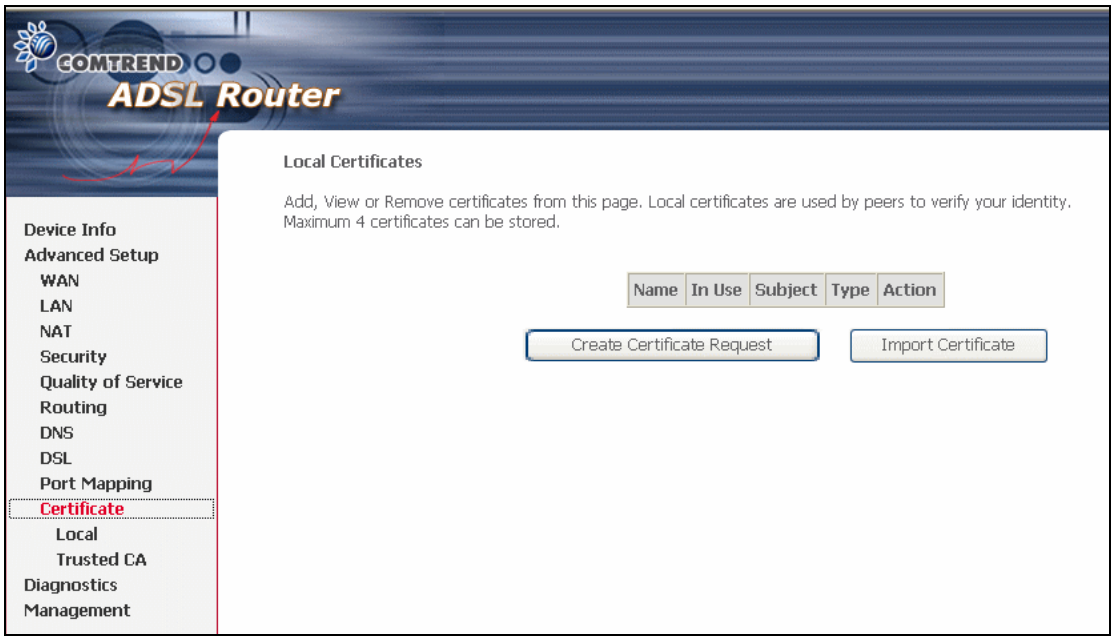
If the setup-box was connected with interface "ETH1" and send a DHCP request with vendor id "Video", CPE DHCP server will forward this request to ISP's DHCP server.
And CPE will change the port mapping configuration automatically. The port mapping configuration will become:

1. Default: ETH2, ETH3, ETH4 and USB.
2. Video: nas_0_36, nas_0_37, nas_0_38 and ETH1.

6.10 Certificate

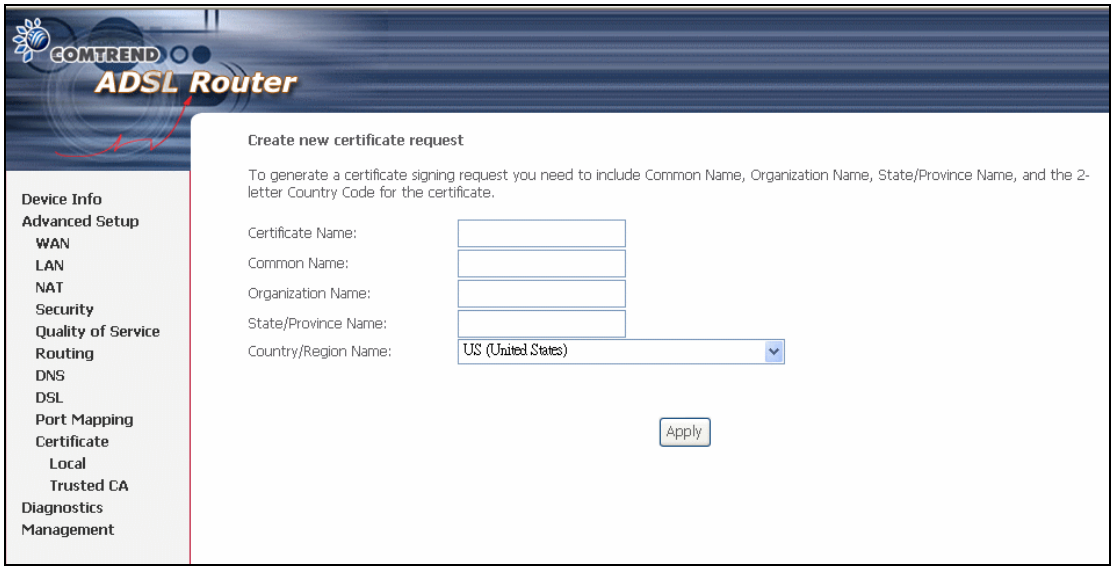
A certificate is a public key, attached with its owner's information (company name, server name, personal real name, contact e-mail, postal address, etc) and digital signatures. There will be one or more digital signatures attached on the certificate, indicating that these signers have verified that the owner information of this certificate is correct.

6.10.1 Local



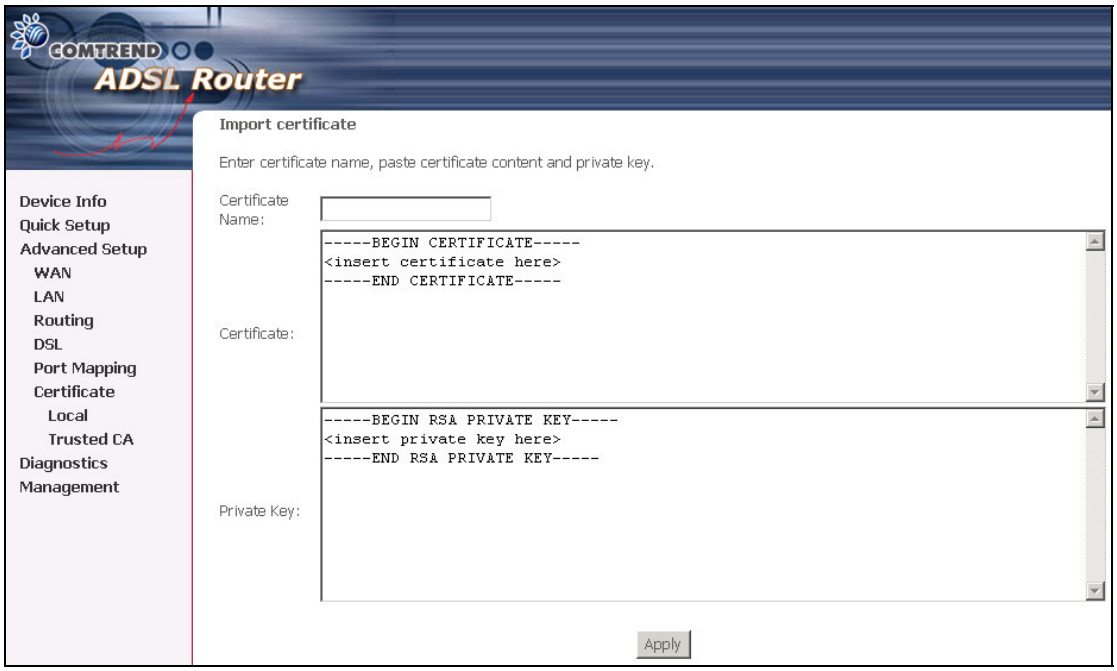
Click **Create Certificate Request** to generate a certificate signing request. The certificate signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate signing request. Actually, your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. The explanation for each column in the following table is only for reference.

Certificate Name	A user-defined name for the certificate.
Common Name	Usually, it is the fully qualified domain name for the machine.
Organization Name	The exact legal name of your organization. Do not abbreviate.
State/Province Name	The state or province where your organization is located. It cannot be abbreviated.
Country/Region Name	The two-letter ISO abbreviation for your country.



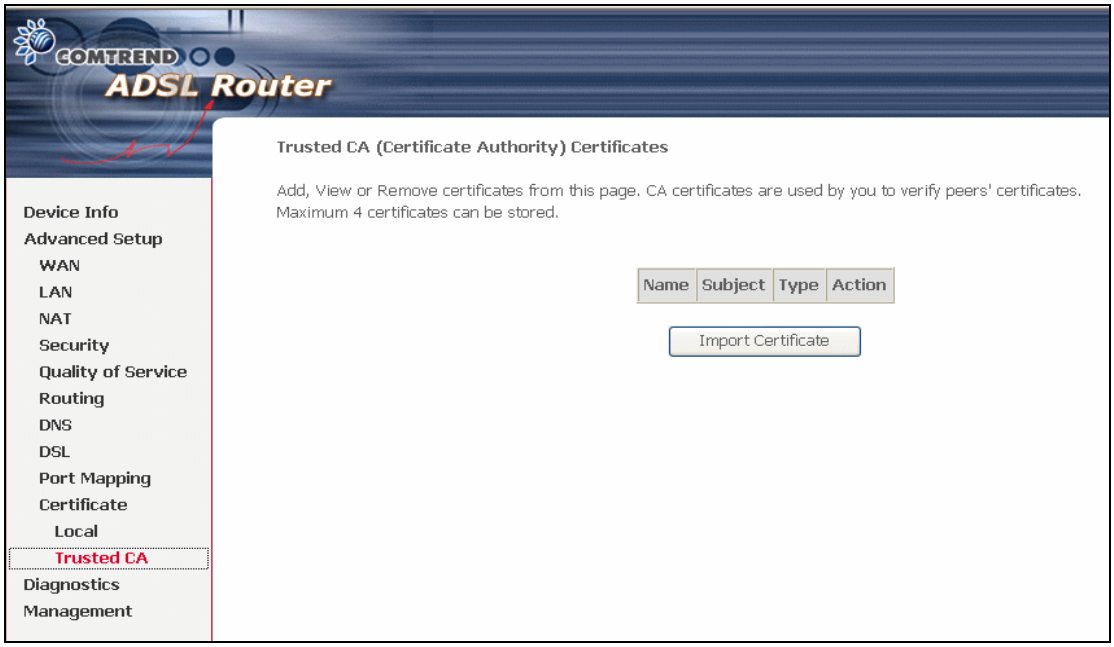
Click **Apply** to generate a private key and a certificate signing request.

This page is used to paste the certificate content and the private key provided by your vendor/ISP/ITSP.



6.10.2 Trusted CA

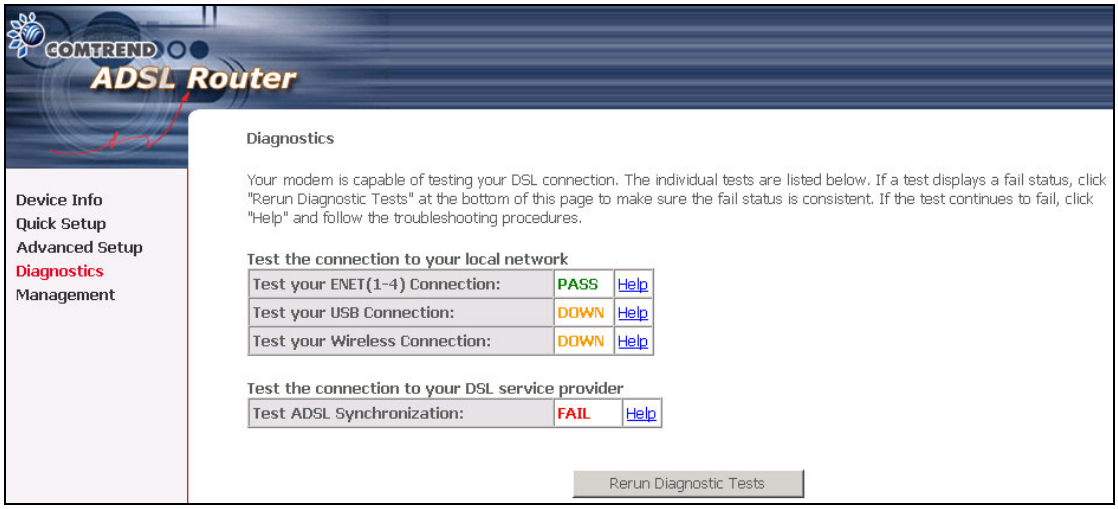
CA is the abbreviation for Certificate Authority. CA is a part of the X.509 system. It is itself a certificate, attached with the owner information of this certificate authority. But its purpose is not to do encryption/decryption. Its purpose is to sign and issue certificates; in order to prove the owner information of that certificate is correct.



Click **Import Certificate** to paste the certificate content of your trusted CA. Generally speaking, the certificate content will be provided by your vendor/ISP/ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.

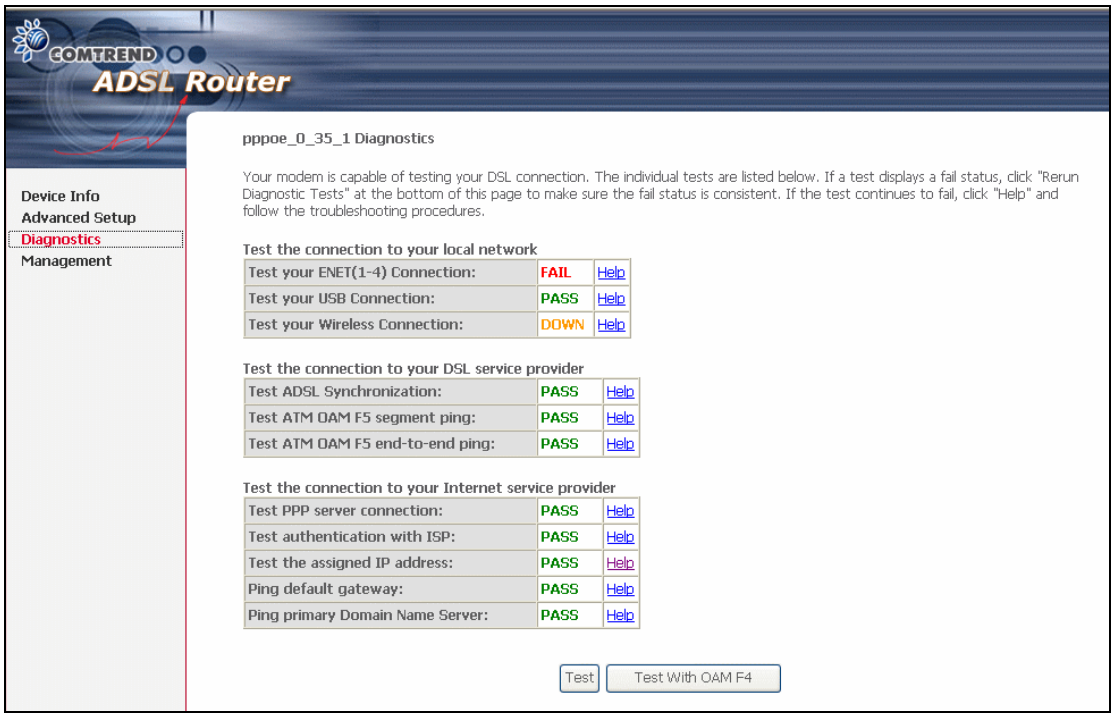
Chapter 7 Diagnostics

The Diagnostics menu provides feedback on the connection status of the CT-5621T and the ADSL link. The individual tests are listed below. If a test displays a fail status, click **Rerun Diagnostic Tests** at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click **Help** and follow the troubleshooting procedures.


COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management
Diagnostics
Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Test the connection to your local network
Test your ENET(1-4) Connection: PASS Help
Test your USB Connection: DOWN Help
Test your Wireless Connection: DOWN Help
Test the connection to your DSL service provider
Test ADSL Synchronization: FAIL Help
Rerun Diagnostic Tests

Test	Description
Ethernet Connection	**Pass:** indicates that the Ethernet interface from your computer is connected to the LAN port of your DSL Router. A flashing or solid green LAN LED on the router also signifies that an Ethernet connection is present and that this test is successful. **Fail:** Indicates that the DSL Router does not detect the Ethernet interface on your computer.
USB Connection	**Pass:** Indicates that the USB interface from your computer is connected to router properly. **Down:** Indicates that the DSL Router does not detect the signal from USB interface.
ADSL Synchronization	**Pass:** Indicates that the DSL modem has detected a DSL signal from the telephone company. A solid WAN LED on the router also indicates the detection of a DSL signal from the telephone company. **Fail:** indicates that the DSL modem does not detect a signal from the telephone company's DSL network. The WAN LED will stop blinking (i.e. training) and the LED will switch off.

Diagnostics screen with a PPPoE configured for your reference.


COMTREND
ADSL Router
Device Info
Advanced Setup
Diagnostics
Management
pppoe_0_35_1 Diagnostics
Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Test the connection to your local network
Test your ENET(1-4) Connection: FAIL Help
Test your USB Connection: PASS Help
Test your Wireless Connection: DOWN Help
Test the connection to your DSL service provider
Test ADSL Synchronization: PASS Help
Test ATM OAM F5 segment ping: PASS Help
Test ATM OAM F5 end-to-end ping: PASS Help
Test the connection to your Internet service provider
Test PPP server connection: PASS Help
Test authentication with ISP: PASS Help
Test the assigned IP address: PASS Help
Ping default gateway: PASS Help
Ping primary Domain Name Server: PASS Help
Test
Test With OAM F4

Chapter 8 Management

The Management section of the CT-5621T supports the following maintenance functions and processes:

- Settings
- System log
- TR-069 Client
- Internet Time
- Access Control
- Update software
- Save/Reboot

8.1 Settings

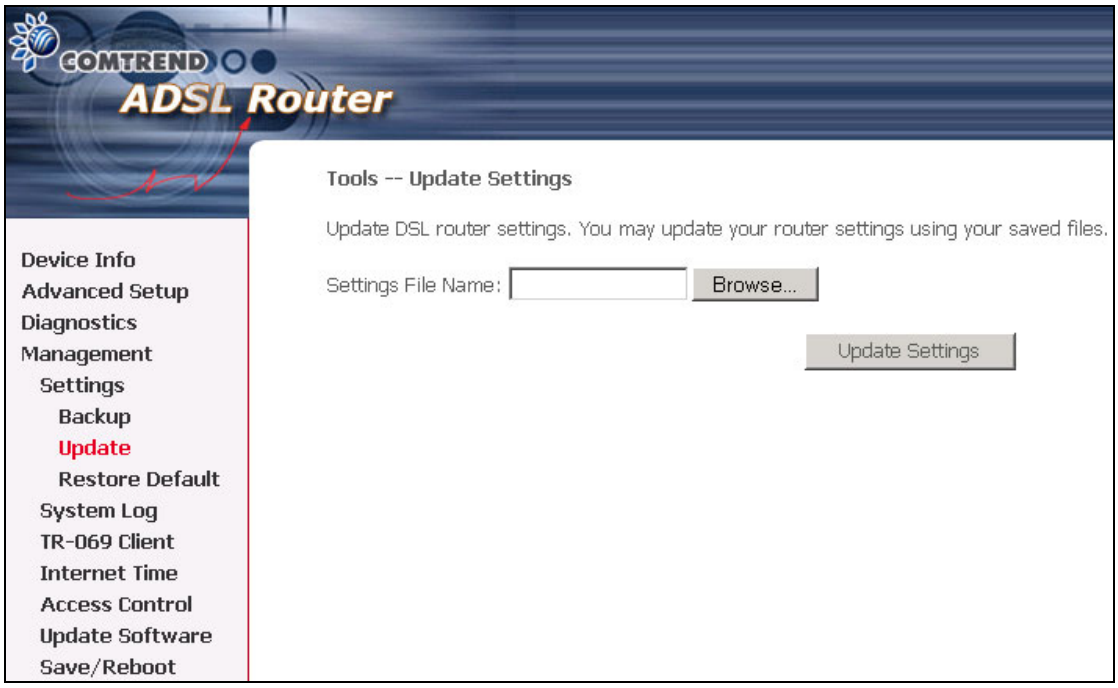
The Settings option allows you to back up your settings to a file, retrieve the setting file, and restore the settings.

8.1.1 Configuration Backup

The Backup option under Management>Settings save your router configurations to a file on your PC. Click BACKUP Settings in the main window. You will be prompted to define the location of the backup file to save. After choosing the file location, click **Backup Settings.** The file will then be saved to the assigned location.

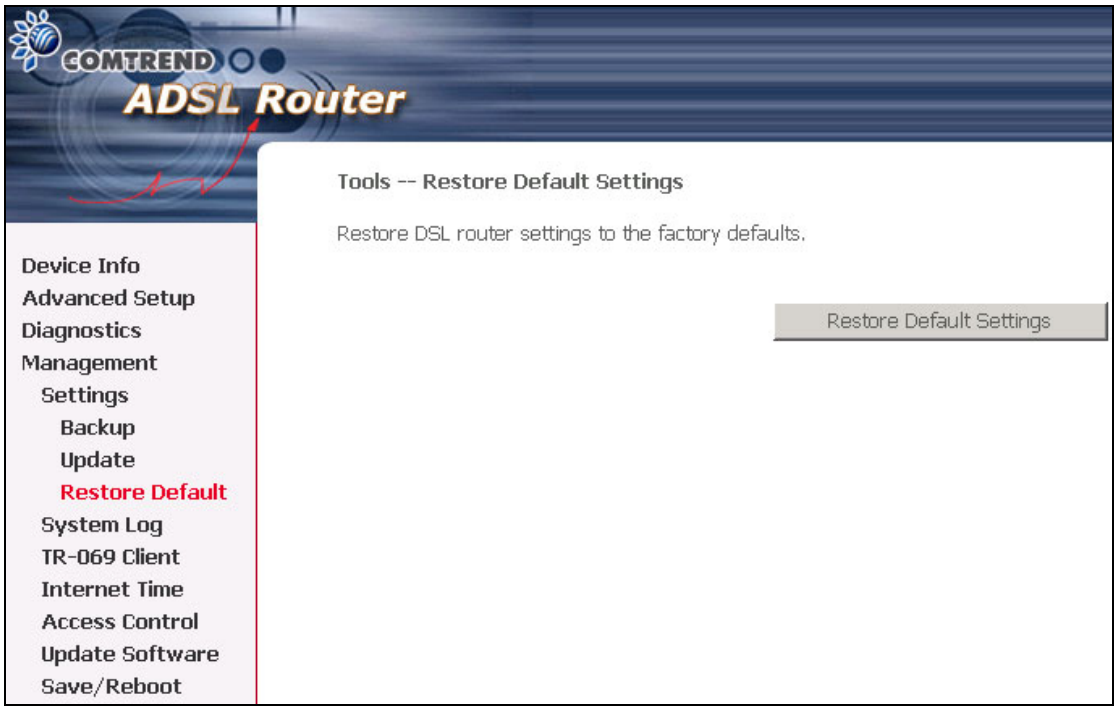
8.1.2 Update Settings

The Update option under Management>Settings update your router settings using your saved files.



8.1.3 Restore Default

Clicking the Restore Default Configuration option in the Restore Settings screen can restore the original factory installed settings.



NOTE 1: This entry has the same effect as the hardware reset-to-default button. The CT-5621T board hardware and the boot loader support the **reset to default** button. If the reset button is continuously pushed for more than 5 seconds, the boot loader will erase the entire configuration data saved on the flash memory.

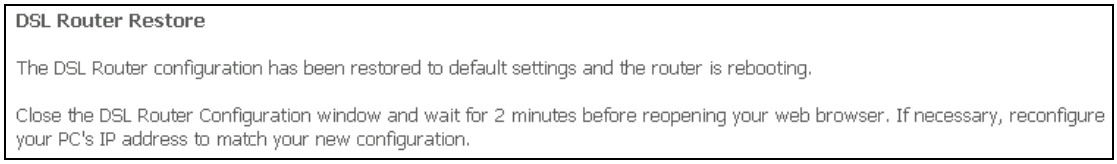
NOTE 2: Restoring system settings requires a system reboot. This necessitates that the current Web UI session be closed and restarted. Before restarting the connected PC must be configured with a static IP address in the 192.168.1.x subnet in order to configure the CT-5621T.

Default settings

The CT-5621T default settings are

- LAN port IP= 192.168.1.1, subnet mask = 255.255.255.0
- Local user name: root
- Password: 12345
- Remote user name: support
- Remote user password: support

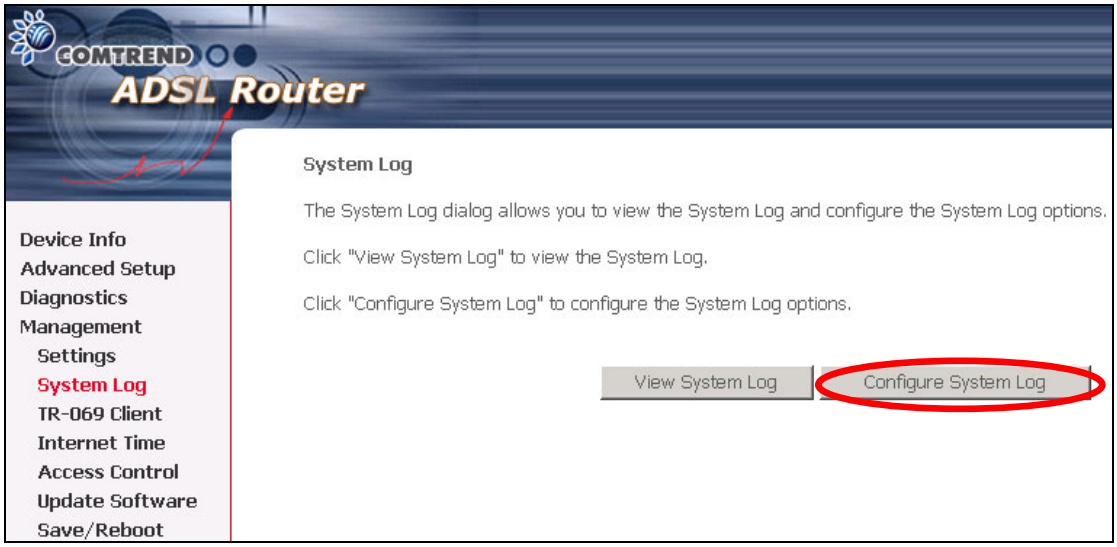
After the Restore Default Configuration button is selected, the following screen appears. Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC IP address to match your new configuration.


DSL Router Restore
The DSL Router configuration has been restored to default settings and the router is rebooting.
Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

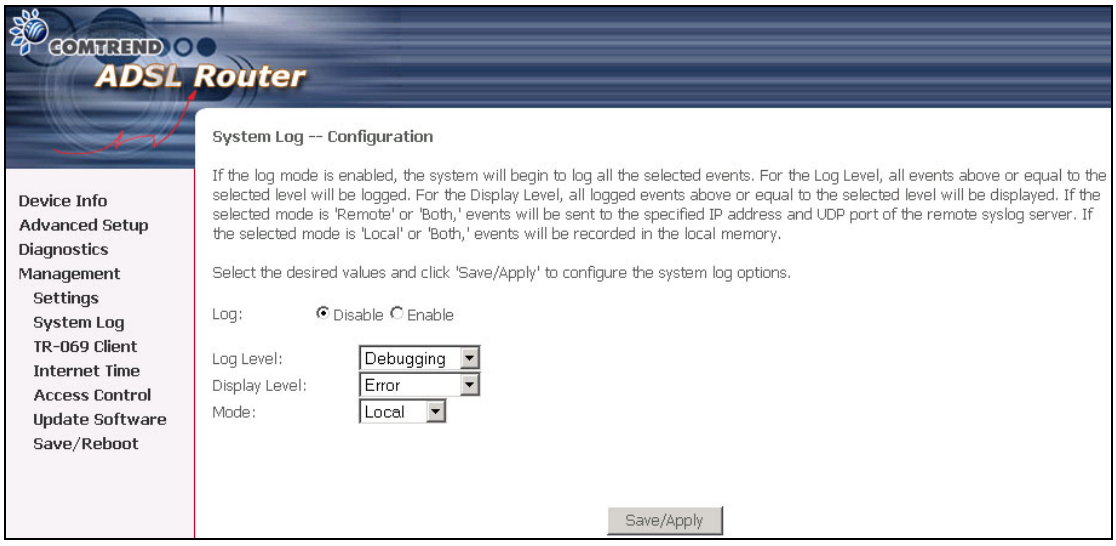
8.2 System Log

The System Log option under Management>Settings allows you to view the system events log, or to configure the System Log options. The default setting of system log is disabled. Follow the steps below to enable and view the system log.

1. Click **Configure System Log** to display the following screen.

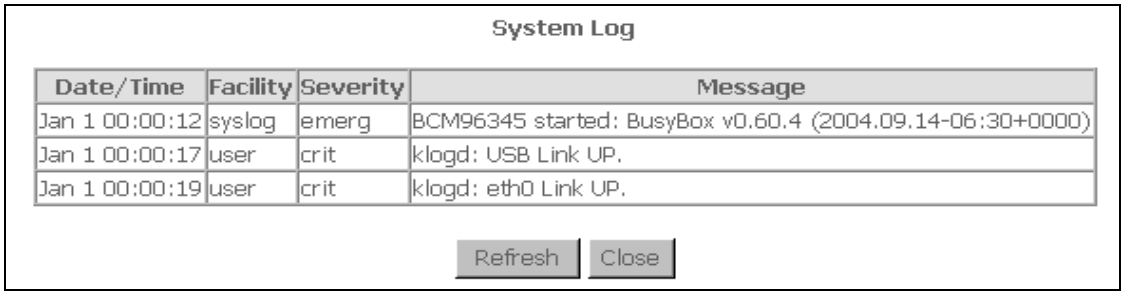


2. Select from the desired Log options described in the following table, and then click **SAVE/Apply**.


COMTREND
ADSL Router
Device Info
Advanced Setup
Diagnostics
Management
Settings
System Log
TR-069 Client
Internet Time
Access Control
Update Software
Save/Reboot
System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Select the desired values and click 'Save/Apply' to configure the system log options.
Log: Disable Enable
Log Level: Debugging
Display Level: Error
Mode: Local
Save/Apply

Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, tick Enable and then Apply button.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the CT-5621T SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging," which is the lowest critical level. The following log levels are ● Emergency = system is unusable ● Alert = action must be taken immediately ● Critical = critical conditions ● Error = Error conditions ● Warning = normal but significant condition ● Notice= normal but insignificant condition ● Informational= provides information for reference ● Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the **View System Log** page for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote syslog server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

3. Click **View System Log**. The results are displayed as follows.

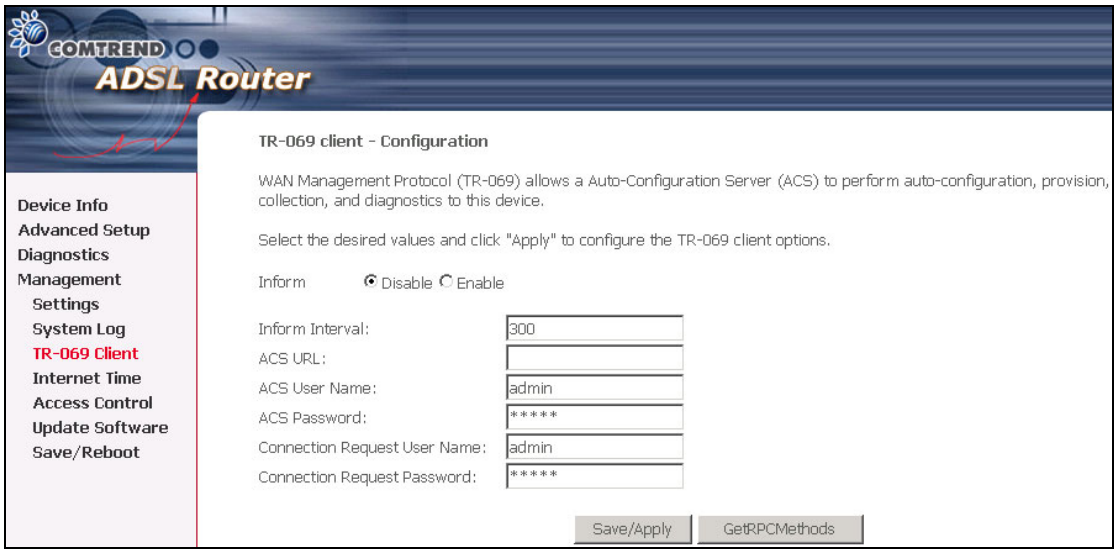

System Log

Date/Time	Facility	Severity	Message
Jan 1 00:00:12	syslog	emerg	BCM96345 started: BusyBox v0.60.4 (2004.09.14-06:30+0000)
Jan 1 00:00:17	user	crit	klogd: USB Link UP.
Jan 1 00:00:19	user	crit	klogd: eth0 Link UP.

Refresh Close

8.3 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

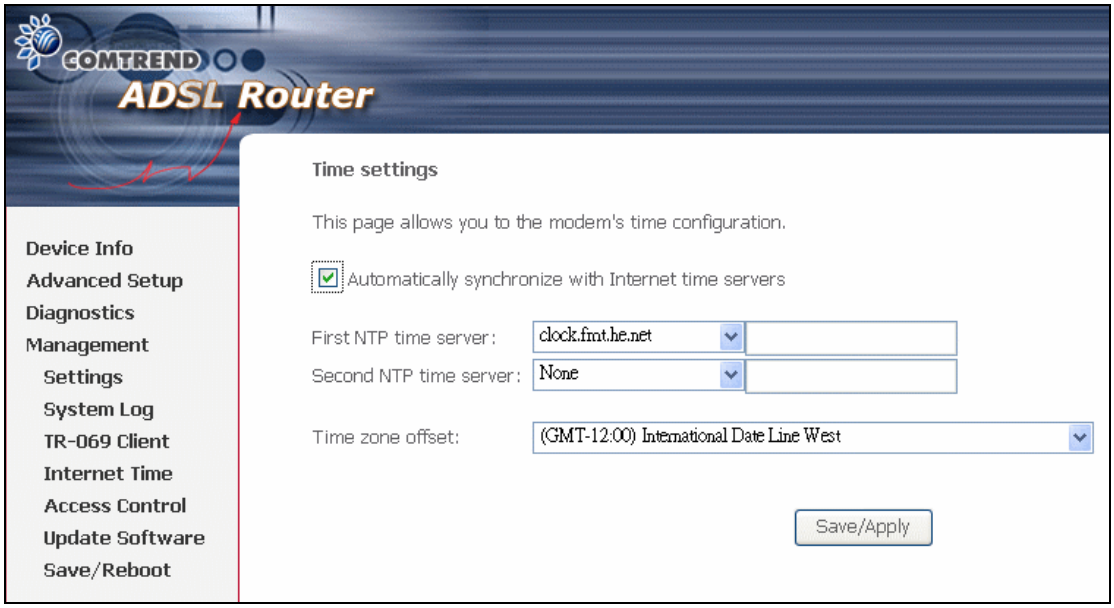


Option	Description
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
Connection Request	Username used to authenticate an ACS making a Connection

User Name	Request to the CPE.
Connection Request Password	Password used to authenticate an ACS making a Connection Request to the CPE.
Get RPC Methods	This method may be used by a CPE or ACS to discover the set of methods supported by the ACS or CPE it is in communication with. This list may include both standard TR-069 methods (those defined in this specification or a subsequent version) and vendor-specific methods. The receiver of the response MUST ignore any unrecognized methods. Click this button to force the CPE to immediately establish a connection to the ACS.

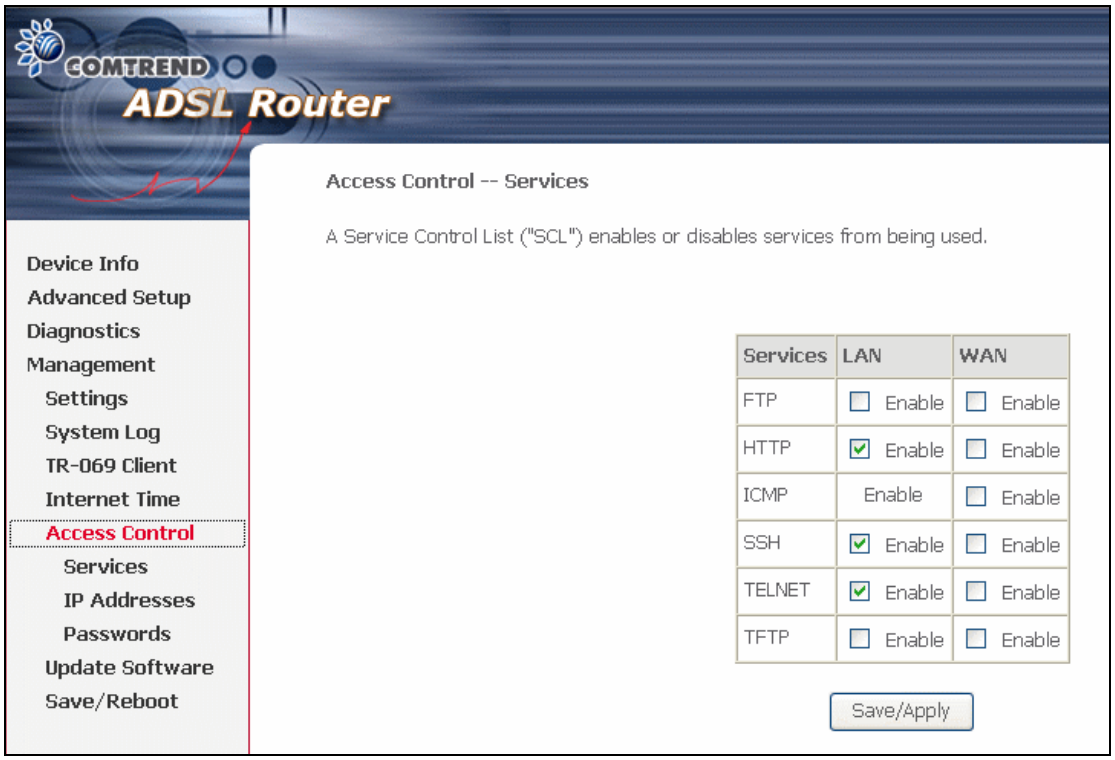
8.4 Internet Time

The Internet Time option under Management menu bar configures the Modem's time. To automatically synchronize with Internet time servers, tick the corresponding box displayed on the screen. Then click **Save/Apply**.



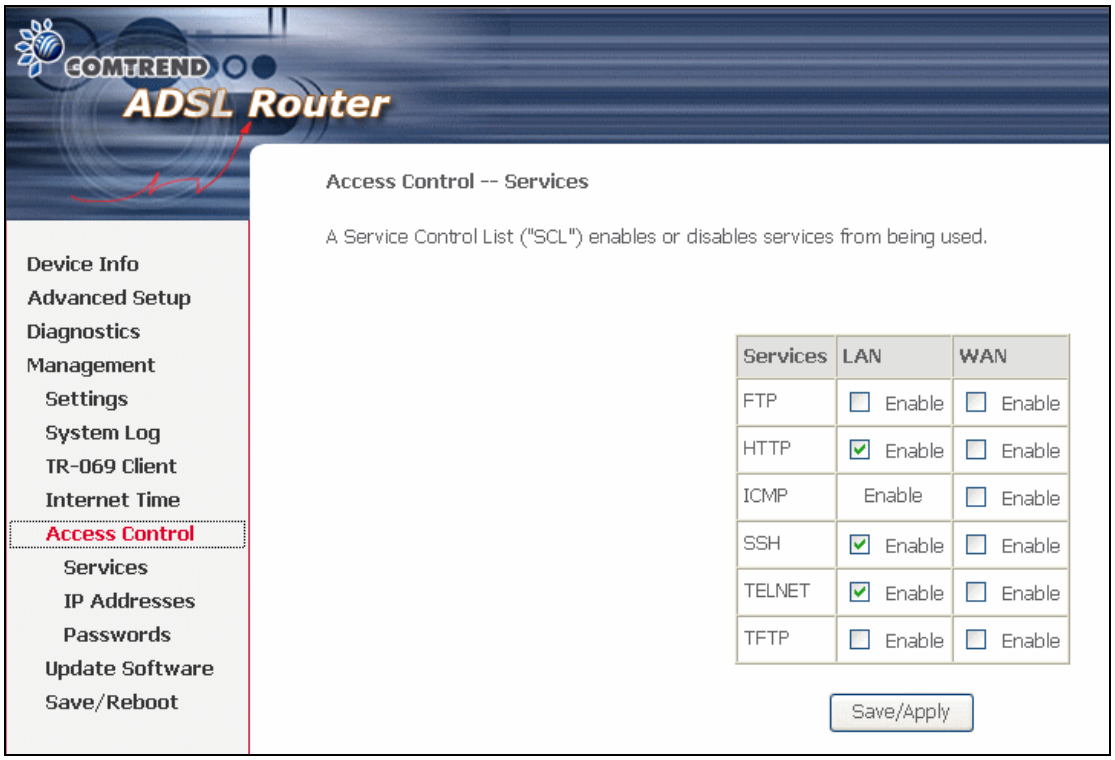
8.5 Access Control

The Access Control option under Management menu bar configures the access-related parameters, including three parts: Services, IP Address, and Passwords.



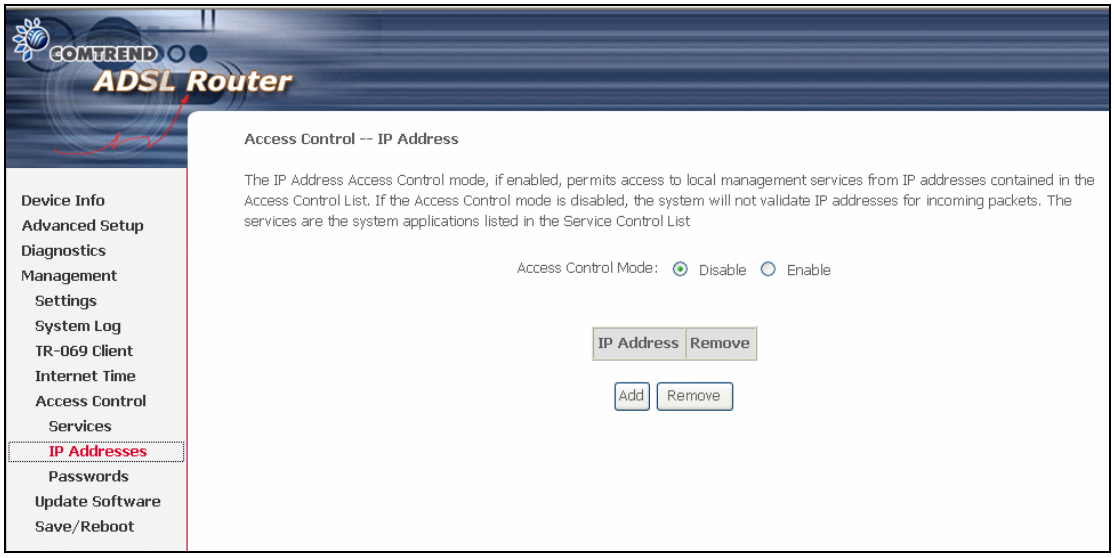
8.5.1 Services

The Services option limits or opens the access services over the LAN or WAN. These services are provided FTP, HTTP, ICMP, SSH (Security Socket Share), TELNET, and TFTP. Enable the service by checking the item in the corresponding checkbox, and then click **Save/Apply**.

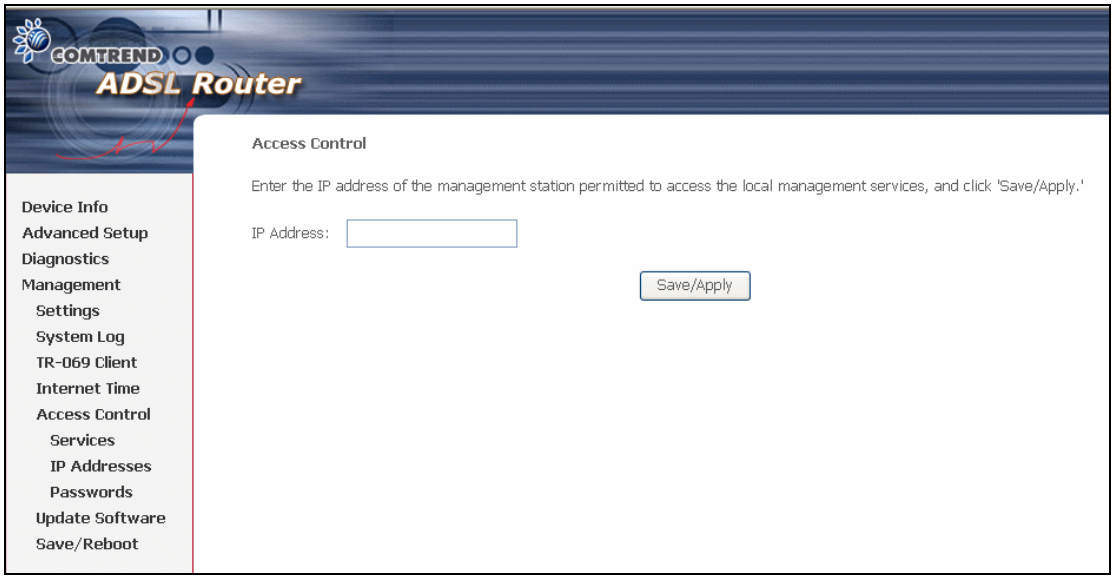


8.5.2 Access IP Addresses

The IP Addresses option limits the access by IP address. If the Access Control Mode is enabled, only the allowed IP addresses can access the router. Before you enable it, configure the IP addresses by clicking the **Add** button.


COMTREND
ADSL Router
Device Info
Advanced Setup
Diagnostics
Management
Settings
System Log
TR-069 Client
Internet Time
Access Control
Services
IP Addresses
Passwords
Update Software
Save/Reboot
Access Control -- IP Address
The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List
Access Control Mode: Disable Enable
IP Address Remove
Add Remove

Enter the IP address, subnet mask and select the interface. Then click **Save/Apply** to allow the PC with this IP address managing the DSL Router.

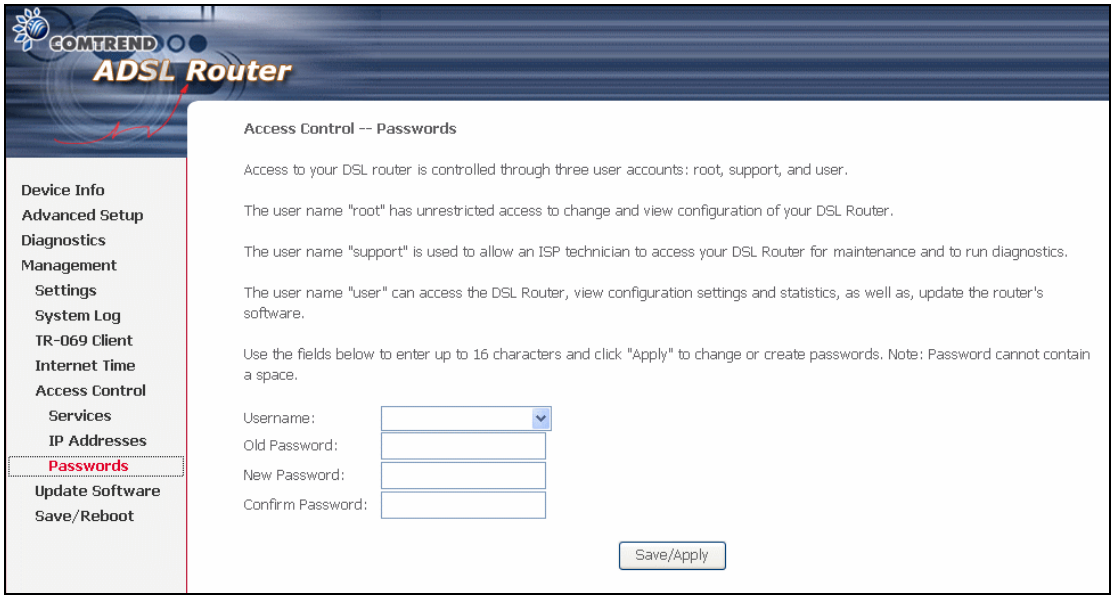


8.5.3 Passwords

The Passwords option configures the access passwords for the router. Access to your DSL router is controlled through three user accounts: root, support, and user.

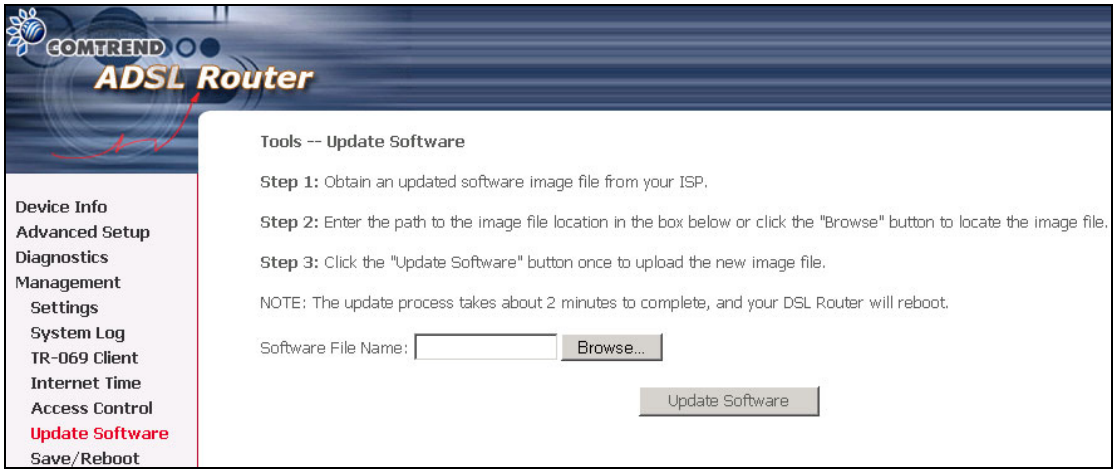
- "root" has unrestricted access to change and view configuration of your DSL Router.
- "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.
- "user" can access the Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click Apply to change or create passwords.


COMTREND
ADSL Router
Device Info
Advanced Setup
Diagnostics
Management
Settings
System Log
TR-069 Client
Internet Time
Access Control
Services
IP Addresses
Passwords
Update Software
Save/Reboot
Access Control -- Passwords
Access to your DSL router is controlled through three user accounts: root, support, and user.
The user name "root" has unrestricted access to change and view configuration of your DSL Router.
The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.
Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.
Username:
Old Password:
New Password:
Confirm Password:
Save/Apply

8.6 Update software

The Update Software screen allows you to obtain an updated software image file from your ISP. Manual software upgrades from a locally stored file can be performed using the following screen.


COMTREND
ADSL Router
Device Info
Advanced Setup
Diagnostics
Management
Settings
System Log
TR-069 Client
Internet Time
Access Control
Update Software
Save/Reboot
Tools -- Update Software
Step 1: Obtain an updated software image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 3: Click the "Update Software" button once to upload the new image file.
NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.
Software File Name:
Browse...
Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the **Browse** button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

8.7 Save and Reboot

The Save/Reboot options saving the configurations and reboot the router. Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC IP address to match your new configuration.

Appendix A: Firewall

Stateful Packet Inspection
Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

Denial of Service attack
Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the device can withstand are: ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack and Tear Drop.

TCP/IP/Port/Interface filtering rules
These rules help in the filtering of traffic at the Network layer i.e. Layer 3.
When a Routing interface is created "Enable Firewall" must be checked.
Navigate to Advanced Setup -> Security -> IP Filtering, web page.

Outgoing IP Filtering: Helps in setting rules to DROP packets from the LAN interface. By default if Firewall is Enabled all IP traffic from LAN is allowed. By setting up one or more filters, particular packet types coming from the LAN can be dropped.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be dropped.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

Destination IP Address/Destination Subnet Mask: Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be dropped.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

Examples:

1. Filter Name : Out_Filter1
   Protocol : TCP
   Source Address : 192.168.1.45
   Source Subnet Mask : 255.255.255.0
   Source Port : 80
   Dest. Address : NA
   Dest. Sub. Mask : NA
   Dest. Port : NA

This filter will Drop all TCP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

2. Filter Name : Out_Filter2
   Protocol : UDP
   Source Address : 192.168.1.45
   Source Subnet Mask : 255.255.255.0
   Source Port : 5060:6060
   Dest. Address : 172.16.13.4
   Dest. Sub. Mask : 255.255.255.0
   Dest. Port : 6060:7070

This filter will drop all UDP packets coming from LAN with IP Address/Sub.Mask 192.168.1.45/24 and a source port in the range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port in the range of 6060 to 7070.

Incoming IP Filtering:

Helps in setting rules to ACCEPT packets from the WAN interface. By default all incoming IP traffic from WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, particular packet types coming from the WAN can be Accepted.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be accepted.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

Destination IP Address/Destination Subnet Mask: Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be accepted.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

The WAN interface on which these rules apply needs to be selected by the user.

Examples:

1. Filter Name : In_Filter1
   Protocol : TCP
   Source Address : 210.168.219.45
   Source Subnet Mask : 255.255.0.0
   Source Port : 80
   Dest. Address :NA
   Dest. Sub. Mask : NA
   Dest. Port : NA

Selected WAN interface: mer_0_35/nas_0_35

This filter will ACCEPT all TCP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub. Mask 210.168.219.45/16 having a source port of 80 irrespective of the destination. All other incoming packets on this interface are DROPPED.

2. Filter Name : In_Filter2
   Protocol : UDP
   Source Address : 210.168.219.45
   Source Subnet Mask : 255.255.0.0
   Source Port : 5060:6060
   Dest. Address : 192.168.1.45
   Dest. Sub. Mask : 255.255.255.0
   Dest. Port : 6060:7070

This rule will ACCEPT all UDP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub.Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC Layer Filtering:
These rules help in the filtering of traffic at the Layer 2. MAC Filtering is only effective on ATM PVCs configured in Bridge mode. After a Bridge mode PVC is created, navigate to Advanced Setup -> Security -> MAC Filtering web page.

Global Policy:
When set to Forwarded the default filter behavior is to
Forward all MAC layer frames except those explicitly stated in the rules.
Setting it to Blocked changes the default filter behavior to Drop all
MAC layer frames except those explicitly stated in the rules.

To setup a rule:

Protocol Type: Can be PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI or IGMP.

Destination MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular destination address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Source MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular source address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Frame Direction:

LAN <=> WAN --> All Frames coming/going to/from LAN or to/from WAN.

WAN => LAN --> All Frames coming from WAN destined to LAN.

LAN => WAN --> All Frames coming from LAN destined to WAN

User needs to select the interface on which this rule is applied.

Examples:

1.

Global Policy: Forwarded

Protocol Type: PPPoE

Dest. MAC Addr: 00:12:34:56:78:90

Source MAC Addr: NA

Frame Direction: LAN => WAN

WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule drops all PPPoE frames going from LAN-side to WAN-side with a Dest. MAC Addr. of 00:12:34:56:78:90 irrespective of its Source MAC Addr. on the br_0_34 WAN interface. All other frames on this interface are forwarded.

2.

Global Policy: Blocked

Protocol Type: PPPoE

Dest. MAC Addr: 00:12:34:56:78:90

Source MAC Addr: 00:34:12:78:90:56

Frame Direction: WAN => LAN

WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule forwards all PPPoE frames going from WAN-side to LAN-side with a Dest. MAC Addr. of 00:12:34:56:78 and Source MAC Addr. of 00:34:12:78:90:56 on the br_0_34 WAN interface. All other frames on this interface are dropped.

Daytime Parental Control

This feature restricts access of a selected LAN device to an outside Network through the router, as per chosen days of the week and the chosen times.

User Name: Name of the Filter.

Browser's MAC Address: Displays MAC address of the LAN device on which the browser is running.

Other MAC Address: If restrictions are to be applied to a device other than the one on which the browser is running, the MAC address of that LAN device is entered.

Days of the Week: Days of the week, when the restrictions are applied.

Start Blocking Time: The time when restrictions on the LAN device are put into effect.

End Blocking Time: The time when restrictions on the LAN device are lifted.

Example:

User Name: FilterJohn
Browser's MAC Address: 00:25:46:78:63:21
Days of the Week: Mon, Wed, Fri
Start Blocking Time: 14:00
End Blocking Time: 18:00

When this rule i.e. FilterJohn is entered, a LAN device with MAC Address of 00:25:46:78:63:21 will be restricted access to the outside network on Mondays, Wednesdays and Fridays, from 2pm to 6pm. On all other days and time this device will have access to the outside Network.

Appendix B: Pin Assignments

Line port (RJ11)

Pin	Definition	Pin	Definition
1	-	4	ADSL_TIP
2	-	5	-
3	ADSL_RING	6	-

Pin Assignments of the RJ11 Port

LAN Port (RJ45)

Pin	Definition	Pin	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

Pin assignments of the LAN Port

Appendix C: Specifications

Rear Panel

RJ-11 X1 for ADSL, RJ-45 X 4 for LAN, USB X 1, Reset Button X 1
Power Jack X 1, Power switch X 1

ADSL

Standard ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2

G.992.5 (ADSL2+).....	Downstream : 24 Mbps	Upstream : 1.3 Mbps
G.992.3 (ADSL2).....	Downstream : 12 Mbps	Upstream : 1.3 Mbps
G.DMT	Downstream : 8 Mbps	Upstream : 832 Kbps

Ethernet

Standard	IEEE 802.3, IEEE 802.3u
10/100 BaseT	Auto-sense
MDI/MDX support	Yes

ATM Attributes

RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE); RFC 1577 (IPoA)

Support PVCs	16
AAL type	AAL5
ATM service class	UBR/CBR/VBR
ATM UNI support	UNI3.1/4.0
OAM F4/F5	Yes

Management

Telnet, Web-based management, Configuration backup and restoration, TR-069, SNMP (optional)
Software upgrade via HTTP, TFTP server, or FTP server

Bridge Functions

Transparent bridging and learning	IEEE 802.1d
VLAN support	Yes
Spanning Tree Algorithm	Yes
IGMP Proxy	Yes

Routing Functions

Static route, RIP, and RIPv2, NAT/PAT, DHCP Server/DHCP Relay, DNS Proxy, ARP

Security Functions

Authentication protocols PAP, CHAP,
TCP/IP/Port filtering rules, Port triggering/Forwarding, Packet and MAC address filtering, access control, SSH

Application Passthrough

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box, etc

OS Supported for USB driver

Windows Vista/2000/XP/ME/98SE

Power Supply

External power adapter110 Vac or 220 Vac

Environment Condition

Operating temperature 0 ~ 50 degrees Celsius
Relative humidity 5 ~ 90% (non-condensing)

Dimensions

200 mm (W) x 44 mm (H) x 136.5 mm (D)

Certifications

FCC Part 15 class B, FCC Part 68, CE

Note: Specifications are subject to change without notice.

Appendix D: SSH Client

Linux OS comes with ssh client. MicroSoft Windows does not have ssh client but there is a public domain one "putty" that you can download.
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

To access the router using Linux ssh client:
From LAN: Use the router WEB UI to enable SSH access from LAN.
(default is enabled)
type: ssh -l root 192.168.1.1

From WAN: In the router, use WEB UI to enable SSH access from WAN.
type: ssh -l support router-WAN-ip-address

To access the router using Windows putty ssh client:
From LAN: Use the router WEB UI to enable SSH access from LAN
(default is enabled)
type: putty -ssh -l root 192.168.1.1

From WAN: In the router, use WEB UI to enable SSH access from WAN.
type: putty -ssh -l support router-WAN-ip-address